Universidade de Aveiro
Departamento de Electrónica, Telecomunicações e Informática,
2013

Diogo Miguel
Augusto Lopes

Acesso à Internet com Handover de Veículos através de Gateways Móveis

Universidade de Aveiro
Departamento de Electrónica, Telecomunicações e Informática,
2013

Diogo Miguel Augusto Lopes

Acesso à Internet com Handover de Veículos através de Gateways Móveis

"The best road to progress is freedom's road."

— John F. Kennedy

Diogo Miguel Augusto Lopes

Acesso à Internet com Handover de Veículos através de Gateways Móveis

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Electrónica e de Telecomunicações, realizada sob a orientação científica da Doutora Susana Sargento, Professora auxiliar do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro e co-orientação do Doutor João Barros, Professor Associado do Departamento de Engenharia Eletrotécnica e de Computadores da Faculdade de Engenharia da Universidade do Porto.

o júri / the jury

presidente / president

Professor Doutor José Alberto Gouveia Fonseca
Professor Associado do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro

vogais / examiners committee

Professora Doutora Ana Cristina Costa Aguiar
Professora Auxiliar Convidada, Departamento de Engenharia Eletrotécnica e de Computadores da Faculdade de Engenharia da Universidade do Porto (Arguente)

Professora Doutora Susana Isabel Barreto de Miranda Sargento
Professora auxiliar do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro (orientadora)

Professor Doutor João Francisco Cordeiro de Oliveira Barros
Professor do Departamento de Engenharia Eletrotécnica e de Computadores da Faculdade de Engenharia da Universidade do Porto (co-orientador)

agradecimentos / acknowledgements

Em primeiro lugar gostaria de agradecer aos meus Pais, Luciano e Clara Lopes, por me terem dado a possibilidade de obter um curso superior, assim como todo o carinho e apoio que me deram ao longo de toda a vida. Gostaria ainda de agradecer à minha namorada Rute por toda a paciência e carinho que teve comigo durante esta àrdua caminhada assim como aos meus amigos e colegas de curso, especialmente ao Rafael e Nuno, com que graças a uma forte amizade e apoio mútuo fomos capazes de nos ajudar a atingir este objectivo. Todos vocês foram a minha força, obrigado.

Agradeço a todos os colaboradores do grupo de investigação NAP que me ajudaram no desenvolvimento desta Dissertação, em especial ao Jorge Dias que me ajudou a melhor perceber o trabalho por si desenvolvido e que serviu assim de arranque ao meu próprio trabalho. Agradeço ainda ao Carlos Frade, Filipe Neves e Carlos Ameixieira pelo apoio prestado ao longo da Dissertação.

Por último, mas não menos importante, gostaria de agradecer à Professora Susana Sargento por primeiramente me ter cativado para a área de redes de telecomunicações e posteriormente pela oportunidade de desenvolver a tese de mestrado numa área tão interessante como é não só a mobilidade como também o próprio projecto em si.

Resumo

A necessidade de estar em permanente ligação com o mundo é já uma realidade na grande maioria dos países; as pessoas querem estar sempre contactáveis, querem estar sempre ligadas ao que se passa à sua volta, na sua cidade, em todo o mundo. Com o forte aumento do número de utilizadores das redes sociais a palavra de ordem da atualidade é partilhar, desde comentários, fotos ou até vídeos, o importante é estar ligado ao mundo.

Também nesse sentido têm vindo a ser desenvolvidas as redes veiculares. Inicialmente pensadas para suportar aplicações de segurança de forma a melhorar o tráfego rodoviário são agora vistas como mais uma forma de proporcionar entretenimento aos seus utilizadores. E a melhor forma de cativar os utilizadores é dar-lhes aquilo que mais utilizam no seu dia a dia, o accesso à Internet. Se os veículos forem capazes de partilhar ligação entre si e para com os seus passageiros, esse será um avanço importante para este tipo de redes.

Contudo, muitos desafios afetam ainda as redes veiculares: prevê-se que tenham uma introdução gradual no mercado, mas lenta, pelo que os primeiros constituintes da rede terão sobretudo de usufruir das ligações já existentes ao longo da estrada, por exemplo, hotspots *WI-FI*. Devido à grande mobilidade dos veículos e consequentemente da rede prevê-se que o número de *handovers* entre pontos de accesso ao longo do trajeto seja elevado. Sem um protocolo de mobilidade apropriado a perda de ligação e sessão seria frequente. De forma a tornar o processo mais transparente para o utilizador é necessário um protocolo de mobilidade de rede capaz de não só fornecer mobilidade ao veículo, como também aos seus passageiros.

O objetivo desta Dissertação de Mestrado centra-se no estudo dos tipos de protocolos de mobilidade já existentes e analisar a possibilidade de os adaptar para redes veiculares e comunicação entre veículos e para os seus passageiros. Neste sentido decidiu-se utilizar como base o protocolo Proxy Mobile IP (PMIPv6) para handover entre estações fixas, e o Nemo - PMIPv6 para handover de redes de veículos entre estações fixas e móveis. Estes mecanismos foram extendidos e implementados para proporcionarem mobilidade numa rede veicular. Para a ligação se manter com a melhor qualidade possível ao longo do trajeto é também necessário uma entidade que monitorize as redes de accesso disponíveis forçando a ligação do sistema à rede que apresentar melhores condições, através de um gestor de ligações.

Os testes efetuados em laboratório e na estrada incidiram sobre as tecnologias de acesso IEEE 802.11p, uma tecnologia desenvolvida especialmente para as redes veiculares, e o IEEE 802.11g, uma das tecnologias mais utilizadas atualmente.

Os resultados de handovers realizados em vários cenários de estrada mostram que os mecanismos desenvolvidos permitem fornecer mobilidade transparente dos veículos e seus passageiros, mesmo em mobilidade entre redes com um número diferente de veículos até à infraestrutura.

Abstract

The need to be always connected to the world is now a reality in most countries; people want to be always reachable, want to be always connected to what is happening around them, in their city, worldwide. With the sharp increase in the number of users of social networks, the watchword of today is to share, from comments, photos or even videos, the important thing is to be connected to the world.

Also in this area, vehicular networks, which have been initially designed to support security applications in order to improve road traffic, are now seen more as a way to provide entertainment to its users. And the best way to engage users is to give them what they use most in their daily life, Internet access. If the vehicles are able to share connection between themselves and with their passengers, this would be a breakthrough for this type of network.

However, many problems still affect the vehicular networks: they are expected to be slowly deployed, so that the first nodes of the network will primarily use the already existing connections along the road, as an example, WI-FI hotspots. Due to the high mobility of the vehicles and hence the network, it is expected a significant number of handovers between access points along the route. Without an appropriate mobility protocol the loss of connection and session would be common. In order to make the process more transparent to the user, a network mobility protocol is required, not only to provide mobility to the vehicle, but also to its passengers.

The aim of this MSc Dissertation focuses on the study of the types of existing mobility protocols and discusses the possibility of adapting them to the vehicular networks and to the communication between vehicles and their passengers. In this regard, it was decided to use the Proxy Mobile IPv6 (PMIPv6) for handover between base stations, and Nemo - PMIPv6 for handover of vehicular networks between fixed and mobile stations. These mechanisms have been extended and implemented to provide mobility in a vehicular network. To keep the link with the best quality possible along the path, it is also required an entity to monitor available access networks forcing the connection to the one that has better conditions, through a connection manager.

The tests performed in the laboratory and on the road focused on the access technology IEEE 802.11p, a technology designed specifically for vehicle networks, and IEEE 802.11g, one of the technologies used today.

The results of handovers performed on various road scenarios show that the mechanisms developed allow to provide transparent mobility for both vehicles and passengers, even in mobility between networks with a different number of vehicles to the infrastructure.

Contents

Contents i

List of Figures v

List of Tables ix

1 Introduction 1

1.1 Motivation . . . 1
1.2 Objectives and Contributions . . . 3
1.3 Document Organization . . . 4

2 State of the Art 5

2.1 Introduction . . . 5
2.2 What are vehicular networks? . . . 6
2.2.1 Main features . . . 6
2.3 Equipment . . . 7
2.4 Network Architecture . . . 8
2.5 Addressing . . . 10
2.6 Network Access Technology . . . 12
2.6.1 Dedicated Short-Range Communications (DSRC) allocated spectrum 12
2.6.2 IEEE 802.11p / WAVE . . . 14
2.6.3 Multi-Technology approach . . . 16
2.7 Routing and Dissemination . . . 17
2.7.1 OLSR . . . 18
2.7.2 Better Approach To Mobile Adhoc Networking (BATMAN) . . . 19
2.7.3 BABEL . . . 19
2.7.4 Density-Aware Zone-based packet forwarding in vehicular networks (DAZL) . . . 19

2.7.5 Comparing the routing protocols . . . 20
2.8 VANETs Applications . . . 20
2.9 Mobility . . . 21
2.9.1 MIPv6 . . . 23
Terminology . . . 24
Operation method . . . 25
2.9.2 PMIPv6 . . . 26
Terminology . . . 26
Operation method . . . 28
2.9.3 NEMO . . . 29
Terminology . . . 29
Operation method . . . 30
2.9.4 PNEMO . . . 31
Operation method . . . 31
2.9.5 N-PMIPv6 . . . 32
Operation method . . . 33
2.10 Chapter Considerations . . . 34

3 Mobility Protocols **37**
3.1 Introduction . . . 37
3.2 Scenarios and Architecture . . . 39
3.3 PMIPv6 Implementation used as a starting point . . . 43
3.3.1 Operation method . . . 43
MAG operation method . . . 44
LMA operation method . . . 47
3.3.2 Modifications in previous work . . . 48
3.4 Interaction between the Wireless technology and the Mobility Protocol . . . 48
3.4.1 The IEEE 802.11p and the Router Solicitation/Advertisement messages . . . 49
3.4.2 The IEEE 802.11p and the Neighbor Solicitation / Advertisement messages . . . 51
3.4.3 The IEEE 802.11g and the sharing of the physical interface . . . 53
3.5 Implementation of the N-PMIPv6 mobility protocol . . . 54
3.5.1 LMA tunnel creation to mMAGs . . . 55
3.5.2 MAG and mMAG Identification . . . 56
3.5.3 MAG configuration from a received Router Advertisement . . . 57

3.5.4 Mobile MAG implementation . . . 57
3.5.5 Handover process . . . 58
3.6 IPv4 over IPv6 Internet . . . 63
3.7 Connection Manager Implementation . . . 64
3.7.1 IEEE 802.11g networks detection and connection module . . . 65
3.7.2 IEEE 802.11p networks detection and connection module . . . 66
3.7.3 Connection Manager operation module . . . 66
3.8 Chapter Considerations . . . 69

4 Evaluation of the Mobility Approach 71
4.1 Introduction . . . 71
4.2 Testbed . . . 72
4.2.1 Equipment Used . . . 72
4.2.2 Testbeds implemented . . . 72
4.3 Methodologies and metrics . . . 74
4.4 Lab Experiments Results . . . 77
4.4.1 Results obtained through the testbed 1 . . . 78
Handover Latency . . . 78
Throughput and Packet Loss . . . 78
Jitter . . . 79
4.4.2 Results obtained through the testbed 2 . . . 79
Handover Latency . . . 80
Throughput and Packet Loss . . . 82
Jitter . . . 83
4.4.3 Results of the IPv4 network broadcast . . . 84
4.5 Road Experiments Results . . . 84
4.5.1 Results obtained through the testbed 1 . . . 86
Handover Latency . . . 86
Throughput and Packet Loss . . . 87
Jitter . . . 87
4.5.2 Results obtained through the testbed 2 . . . 87
Handover Latency . . . 87
Throughput and Packet Loss . . . 88
Jitter . . . 90
4.6 Chapter Considerations . . . 90

5 Conclusions and Future Work **94**
5.1 Conclusions 94
5.2 Future work 96

Bibliography **97**

List of Figures

2.1 On Board Unit 9
2.2 VANETs Architecture [21] 10
2.3 Future Intelligent Transport System [32] 13
2.4 DSRC channel allocation [29] 13
2.5 WAVE Protocol Stack [12] 15
2.6 OLSR MPRs operation 18
2.7 Emergency Braking Message 21
2.8 Traffic Lights Applications 21
2.9 MIPv6 Arquitecture [11] 26
2.10 PMIPv6 Arquitecture [43] 28
2.11 NEMO Arquitecture [43] 30
2.12 PNEMO Arquitecture [43] 32
2.13 N-PMIPv6 Arquitecture [43] 33

3.1 Horizontal network handover between RSUs using the IEEE 802.11p 40
3.2 Vertical network handover between RSU and Access Point 41
3.3 Horizontal handover between Access Points at different number of hops . . 41
3.4 Horizontal handover between RSU at different number of hops 42
3.5 Interaction between the N-PMIPv6 and the connection manager 43
3.6 MAG operation flow diagram 45
3.7 LMA operation flow diagram 47
3.8 Router Solicitation problem 50
3.9 Router Solicitation problem solution 51
3.10 Neighbor Solicitation problem 52
3.11 Neighbor Solicitation problem solution 53
3.12 LMA multi tunnel problem 56
3.13 Mobile MAG operation flow diagram 59

3.14 N-PMIPv6 network abstraction 60
3.15 PMIPv6 handover representation 61
3.16 N-PMIPv6 mMAG handover representation 62
3.17 N-PMIPv6 (mMAG and dependent network) handover representation . . . 62
3.18 Path to MNN before handover 63
3.19 Path to MNN after handover 63
3.20 IPv4 Internet enabling system 64
3.21 Connection manager operation flow diagram 68

4.1 In Lab Testbed 1 74
4.2 Real Scenario Testbed 1 74
4.3 In Lab Testbed 2 75
4.4 Real Scenario Testbed 2 75
4.5 RSU 1 76
4.6 RSU 2 / OBU 2 76
4.7 OBU / Vehicle 77
4.8 Handover Latency (tb1-lab) 79
4.9 Detail of figure 4.8 79
4.10 Packet Loss (tb1-lab) 79
4.11 Throughput (tb1-lab) 80
4.12 Jitter (tb1-lab) 81
4.13 Handover Latency (tb2-lab) 82
4.14 Detail of figure 4.13 82
4.15 Packet Loss (tb2-lab) 82
4.16 Throughput (tb2-lab) 83
4.17 Jitter (tb2-lab) 85
4.18 Capture from the video 86
4.19 Handover Latency (tb1-road) 86
4.20 Detail of figure 4.19 86
4.21 Packet Loss (tb1-road) 87
4.22 Throughput (tb1-car) 88
4.23 Jitter (tb1-car) 89
4.24 Handover Latency (tb2-road) 90
4.25 Detail of figure 4.24 90
4.26 Packet Loss (tb2-road) 90
4.27 Throughput (tb2-car) 91

4.28 Jitter (tb2-car) 92

List of Tables

4.1 Technology Handover Cases 73

Chapter 1

Introduction

1.1 Motivation

Nowadays communication has reached a fundamental role in society. Most people cannot leave disconnected of the rest of the world, want to be able to chat and surf on the Internet wherever they are, always with the best connection available. The deployment of the 4G networks allows users to access Internet in most places, but it still has some gaps, like the high costs, and the reduced number of devices with 4G capabilities. WI-FI hotspots have been spread all over the major cities and help users to have better connection speeds; however, WI-FI has some limitations like the lack of handover capabilities, the short range, and the significant time for scanning and access through the available channels.

With this constant connectivity trend, people will increase their traffic everywhere, including in the vehicles. Moreover, connectivity in the vehicles can also give support to other new services. For example, an efficient method for intelligent traffic control is needed in order to achieve better road safety and improvement of traffic flow. With an adequate communication network covering the transportation network, it will be possible to advise the drivers which should be the best road to take in order to avoid traffic congestion, and it will be able to disseminate warning messages such as accident alerts to the nearby cars so that the drivers proceed more carefully. This network, once deployed, can also be used to provide Internet access and entertainment contents to the users inside the vehicle.

Joining these two needs raises one solution, the Vehicular Ad-hoc Networks (VANETs). The concept used is similar to the one applied on ad-hoc networks: vehicles act as mobile nodes carrying a device called On Board Unit (OBU), which has one or several wireless technologies, such as WI-FI (IEEE 802.11a/b/g), WAVE(IEEE 802.11p) or LTE (4G), and connects to other nearby nodes (vehicles) sharing contents or spreading messages.

The nodes should also be able to connect to stationary providers along the road, such as IEEE 802.11p Road Side Units (RSUs) or WI-FI Access Points (APs), which will provide them access to the Internet.

With the deployment and spreading of the VANETs, users will be a little closer to the main objective that is the Always Best Connected (ABC), which refers to the target of keeping always the best connection available for the user performing all the horizontal/vertical handovers (without loss of connection or open accounts) that are needed to always keep the best connection to the services and users, without impact on the running services.

Due to the high mobility of the vehicular networks, it is imperative that the OBUs will be able to provide seamless handover between the access points along the road. While the vehicle is going over the road, the users will want to keep access to the Internet and entertainment applications without the need of reselecting a connection, or reintroducing the credentials in their favorite sites/applications, and therefore, the vehicle as well as its passengers needs to be able to keep their IP addresses stable and unchanged. Mobility has already been the target of several studies in different scenarios and technologies, but this is still a green area on the vehicular networks, especially due the new developed access technology, the WAVE, in which most of the mobility protocols still have not been evaluated.

On a first approach, it is important to allow the vehicles mobility between the fixed access points along the road, since they will be their point of attachment towards the Internet. A mobility protocol capable of providing such characteristics has already been tested on a vehicular scenario in our group in [11]. This work has proven that the Proxy-Mobile IPv6 (PMIPv6) protocol is capable of providing mobility to the vehicles moving along the road, and changing their attachment points between the available fixed infrastructures or even through a 3G connection. It has also demonstrated that the WAVE protocol is the most suitable access technology to be used in the VANETs, since it provides seamless handover capabilities without loss of packets. However, this protocol cannot support network mobility and, as it is an IPv6 mobility protocol, it does not have any support for IPv4 mobility.

Moreover, the scenarios we envision are more complex. When a vehicle moves along the road, it is not intended to just be a user of the available fixed access points; it has also to be able to connect to an access point and then share that connection with other vehicles or its passengers. Cars are not supposed to work as users, but as routers and mobile routers capable of spreading the Internet connection not only to its passengers, but also to the other vehicles nearby. This will allow extending the range of the Internet access connection through multi-hop over the vehicular network reducing the need of fixed infrastructures, and therefore, the costs of deploying a vehicular network. Therefore, a mobility

protocol capable of providing mobility to the vehicles and all their dependents is needed, and PMIPv6 is not capable of performing this role: a network mobility protocol needs to be implemented and adapted to the unique characteristics of the vehicular networks, as well as to the main access technology in use, the IEEE 802.11p/WAVE.

That is the motivation for this MSc Dissertation.

1.2 Objectives and Contributions

Due to the high node mobility of VANETs, it is needed an efficient mechanism capable of providing each node a stable connection to the network independently of the nodes position or density. Maximizing the coverage of the available RSUs is also a priority in order to reduce the cost of the VANETs deployment. To achieve this, a mobility protocol capable of chaining vehicles, and extending the coverage of the RSUs link, will be designed, implemented and tested. With this goal in mind the present Dissertation has the following objectives:

- `Study the propsed mobility protocols`: in order to find the most suitable of being applied on vehicular networks.
- `Network mobility protocol implementation`: adapt the selected protocol in order to support network mobility as well as install and test it on the available testbed.
- `Connection manager implementation`: in order to optimize the handover procedure, it is required an entity capable of monitoring the available networks. It shall identify the best network available and trigger the handover whenever needed.
- `Integrating with real world networks and devices`: adapt the selected protocol in order to support mobility of both IPv4 and IPv6 terminals and also provide them real access to the Internet.
- `Adaptation of the mobility protocol to work over IEEE 802.11p`: the protocol developed needs to be adapted to deal with the unique characteristics of the IEEE 802.11p access technology, such as session establishment procedures and control messages processing, which works differently from the IEEE 802.11g, with which most of the protocols are usually tested.
- `Evaluation of the implemented mobility protocol`: evaluate the network mobility protocol on real world scenarios in order to validate is correct operation.

The work developed on this Dissertation will originate a scientific paper to be submitted in the Summer 2013.

1.3 Document Organization

This Dissertation is organized as follows:

- `Chapter 1`: presents the Dissertation contextualization, the motivation, the framework and the objectives.
- `Chapter 2`: presents the state of the art of the vehicular networks, the mobility protocols and their possible application on VANETs.
- `Chapter 3`: describes the architecture to be studied, the mobility protocol selected as basis, the approach used to implement the network mobility protocol, and the developed connection manager.
- `Chapter 4`: depicts the testbeds used to test the mobility protocol implemented. Then, it presents and discusses the results obtained in the laboratory and on the real road environment tests.
- `Chapter 5`: summarizes all the work that has been performed during this Dissertation. It also suggests possible future improvements to continue the work already done.

Chapter 2

State of the Art

2.1 Introduction

In order to fulfill the objectives of this Dissertation, it is important to review and analyze the work currently done related to this area of study. Therefore, in this chapter it will be introduced the VANETs and a special attention will be given to the mobility protocols. The chapter organization is as follows.

Section 2.2 will introduce the vehicular networks, usually called VANETs, and its main features.

Section 2.3 will present the equipment needed to deploy a vehicular network, from the support of fixed infrastructures to the on board units added to the vehicles.

Section 2.4 will introduce the main network architectures of the VANETs and its main characteristics.

Section 2.5 will present the addressing method adopted on the VANETs and some of the features it should enhance on the future in order to improve the efficiency of the network.

Section 2.6 will introduce the network access technologies which are most suitable for use on VANETs. It will be detailed the Dedicated Short Range Communications technology, the IEEE 802.11p (WAVE), and the possibility of using multi-technology systems in order to take advantage of the highly spreaded cellular and WI-FI networks.

Section 2.7 will present the routing and dissemination characteristics suitable for this type of networks, as well as the routing protocols which may be applied.

Section 2.8 will introduce the main applications for VANETs and some of its advantages.

Section 2.9 will introduce the mobility theme, and will detail the mobility protocols available and its features, in order to find the most suitable one for VANETs.

Finally, section 2.10 will present the chapter considerations resuming the full chapter

and introducing the following one.

2.2 What are vehicular networks?

Vehicular networks, also known as VANETs, are a real life application of ad-hoc networks, where the network is spontaneously formed between nearby vehicles, which are equipped with wireless interfaces that can be of equal or different technologies. This allows communications between nearby vehicles and between vehicles and nearby structures, these structures are usually composed as Road Side Units (RSUs).

The vehicles present in the network can either be private (personal cars) or public (transportation systems, for example buses) and the service providers over the network can be either governmental or private network providers.

2.2.1 Main features

VANETs have some special behavior and characteristics that make them a novel class of wireless networks. These are as follows:

- `Unlimited Power Source`: since the equipment required in cars, the OBUs, are powered by the cars, this type of networks does not usually suffer from power issues on the mobile nodes (vehicles).

- `Higher computer capacity`: there are not relevant size constraints regarding the mobile nodes, so the OBUs can afford better (usually larger) components.

- `Predictable mobility`: as the vehicles are (usually) confined to the roads and using the existent positioning systems, such as GPS, it is possible to predict where the vehicle (mobile node) is heading based on its speed and direction combined with the road information.

However, VANETs face a lot of challenges too, such as:

- `Potentially large scale`: Ideally every vehicle should have is own OBU and behave as a mobile node. This means that the entire transport systems network will turn into a wireless communications network.

- `High mobility`: as the vehicles are the mobile nodes of the network, it is possible to have low density, for example on the highway where relative speed also represents a

challenge, since it can easily go over 300km/h, but it is also possible to have a really high node density, for example, on the rush hour in the cities.

- `Partitioned network`: The highly dynamic nature of the VANETs may result in large inter-vehicle gaps in sparsely populated scenarios, which will lead to several isolated clusters of nodes.

- `Network topology and connectivity`: VANETs are highly dynamic networks, the vehicles are moving and changing their position constantly and they connect and disconnect a lot often which leaves the network topology in constant modifications.

2.3 Equipment

In order to build a wireless communications network over the transports network that already exists, it will be needed the appropriated equipment on the vehicles, the On Board Units (OBUs); it will also be needed to provide fixed infrastructures close to the main roads in order to improve the communication towards the Internet and to extend the range of the network in situations of low vehicle density on the area, the Road Side Units (RSUs). According to Kihl [36] the OBU should have the following components:

- `A Central Processing Unit (CPU)`: which will run and process all the communications protocols and applications needed.

- `Antennas`: which are required to receive and send information at different frequencies depending of the protocol in use at the moment.

- `A GPS receiver`: which will be useful to acquire synchronization with the other OBUs, and some extra information about the vehicle such as position, speed and direction.

- `Sensors`: which are required to acquire extra information about the surroundings.

- `An input/output interface`: which will allow users to access the system.

The RSU will be similar to the OBU, except that it should have a physical connection to fixed network (cable or fiber).

Our group has developed a system capable of providing the required features [3]. It comprises the components described below and identifiable in figure 2.1:

- PCEngines Alix3D3 Module with a 500 MHz AMD Geode LX800, 32-bit x86 architecture, 256 MBytes of memory and Ethernet connection.
- DSRC/WAVE Module compliant with IEEE 802.11p.
- WI-FI Module compliant with IEEE 802.11b/g.
- Omnidirectional L-Com Antenna prepared for frequencies between 5.150 and 5.9 GHz, with a 5dBi gain.
- Omnidirectional antenna prepared for frequencies in the range of 2.4 GHz, with a 5dBi gain.
- Linux Debian (squeeze) Operating system, with the 2.6.32 kernel compiled with the options to support mobility protocols.
- Driver ath5k modified to support the IEEE 802.11p/1609.x [3].
- GPS GlobalTop (MediaTek MT3329).

The main feature of this device is the inclusion of hardware and software capable of supporting the WAVE communication standards, i.e., the IEEE family of standards IEEE 802.11p 1609.x. Thus, using the communications interface corresponding to these standards, it contains the following characteristics:

- Wave fast association.
- Support for the WAVE Short Message Protocol.
- Existence of Control Channel (CCH) and Service Channel (SCH) and support for operations with channel switching.

2.4 Network Architecture

The network architecture is still in discussion: on one hand the introduction of the RSUs will improve the connectivity of the network nodes; but on the other hand, it has large costs associated. According to Lee et all [47], and as can be seen in figure 2.2, there are three architectures possible:

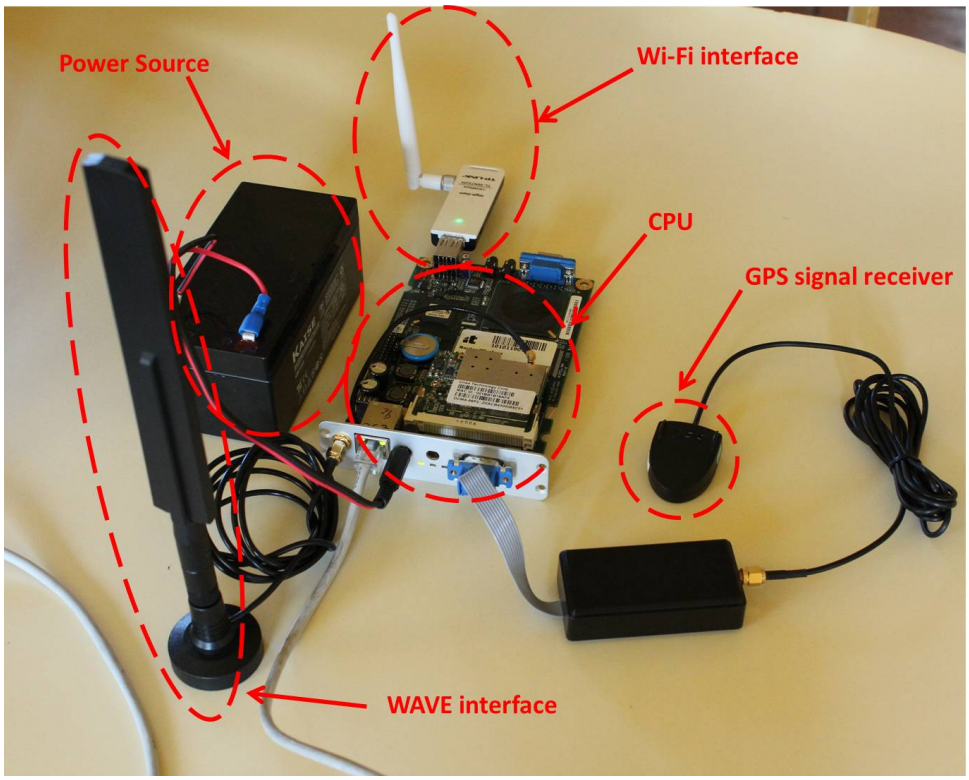


Figure 2.1: On Board Unit

- `Ad-hoc architecture` where the vehicles act like the nodes of a common Ad-hoc network. This means that the vehicles can route the information between themselves by multi-hoping. This architecture main advantage is that it does not require any fixed infrastructures like the RSUs which will reduce the costs. However, the network connectivity is highly dependent of the nodes (vehicles) density, in roads with low vehicles density it will be hard to maintain a stable connection (for example, in highways during the night). Other limitation is that the VANET will not be connected to external networks, and therefore an Internet connection will not be available.

- `WLAN/Cellular architecture`: where fixed infrastructures are disposed over the roads allowing vehicles to connect to them, and routing their information between nodes and also providing them with Internet access. This architecture ensures that the nodes will always be connected; however, the need of full road coverage of RSUs makes the costs rise rapidly. Considering the cellular network for instance, another issue is that the bandwidth is limited and the costs for the user can be too high.

- `Hybrid architecture`: this architecture tries to combine the previous two in order to compensate their disadvantages. Fixed infrastructures should be deployed in strategic points over the roads, based on traffic flow and area coverage for example, in order to help maintain connection between vehicles, and allowing them to access the Internet and also share that access. When there are not nodes in range and neither are RSUs, the mobile node can use the cellular network access to acquire connection, but only as a last resource to prevent extra costs to the user.

Figure 2.2: VANETs Architecture [21]

2.5 Addressing

For most of the applications to be used on the vehicular networks, it is needed an addressing method. Since most of the vehicular networks can be classified as an ad-hoc network, then an addressing scheme of this type of networks should be applied. The addressing method could be static, if the mobile node has just one address which is assigned to him when it connects to the network, or could geographic, which means that the mobile

node address changes when the mobile node changes its physical position. The address scheme can also use other types of relevant information on the address assignment, such as the road identification, direction and speed of the vehicle, vehicle physical information or even driver information such as the level of his driving skills [36].

As the VANETs are ad-hoc networks, Kihl [36] suggests the use of the same protocols applied on MANETs, which are also ad-hoc networks; therefore, and according to Mohsin and Prakash [35], the protocol for assigning IP addresses should meet the following requirements:

- At any given instant of time there should not be two or more nodes with the same IP address, to prevent duplicated IP addresses.
- An IP address should be assigned only for the duration the node stays in the network and become available for assignment to other nodes after it leaves.
- When the whole network has run out of its available IP addresses, it should be denied an IP address to a new node.
- The protocol should handle network partitioning and merging. When two different partitions merge, there is the possibility that two or more nodes have the same IP address. Such duplicate addresses should be detected and resolved.
- The protocol should make sure that only authorized nodes are configured and granted access to network resources.

According to Chlamtac et al. [8], the addressing methods can also be divided in:

- `Static addressing`: when a node enters a network, it gets an IP address and maintains it until it leaves the network. This is the most common addressing scheme in use in the Internet nowadays, and most of the existing ad-hoc network protocols assume this scheme.
- `Geographical addressing`: each node receives an address which depends on its geographical position and it changes as the node moves. The address can translate many kinds of information, such as, direction, speed, type of vehicle and road identification or even drivers characteristics.

Due to the high mobility of the nodes on the vehicular networks, the time required for obtaining an IP address should be as reduced as possible. To deal with this problem Fazio

et al. [20] have proposed a new addressing protocol, the Vehicular Address Configuration (VAC) which intends to improve the performance of the process through the dynamic election of a leader which will act as a Dynamic Host Configuration Protocol (DHCP) server for the other vehicles, and has been demonstrated that it actually reduces the IP acquisition time.

Another solution has been proposed by Nesargi and Prakash [38]. They propose a distributed solution in which, when a node enters the network, it communicates that to all the other nodes through a broadcasted message. Then a node proposes an IP address and, if every other node accepts it, then the new node acquires that address. If the IP address proposed is not accepted, the procedure is repeated until an address is accepted. This is a simple solution, but it uses broadcast messages which may introduce a large overhead on the network due the flooding of those messages.

2.6 Network Access Technology

Nowadays, there are various communication technologies that can be used for network access by the applications running over the vehicular networks. All of these standards have advantages and disadvantages depending on the type of application and the scenarios considered. In vehicle communication systems it is expected that they will have problems in the radio channels, since either the transmitter or the receiver are in motion, and possibly towards each other.

In figure 2.3 it is represented the main idea of a future intelligent transportation system. We will now introduce the main network access technologies involved (developed specifically for this kind of applications).

2.6.1 Dedicated Short-Range Communications (DSRC) allocated spectrum

In 1999 the FCC allocated 75MHz of the spectrum on the frequency of 5.9GHz to the communications V2V e V2I in order to improve the safety and the road traffic and also every kind of private services like the Internet access, which is intended to encourage the adoption of the technology and boost its development.

The DSRC band is a free band (without any charges for the users) like the one of the 2.4GHz or the 5GHz.

The DSRC spectrum is divided into seven channels of 10MHz each, the Control Chan-

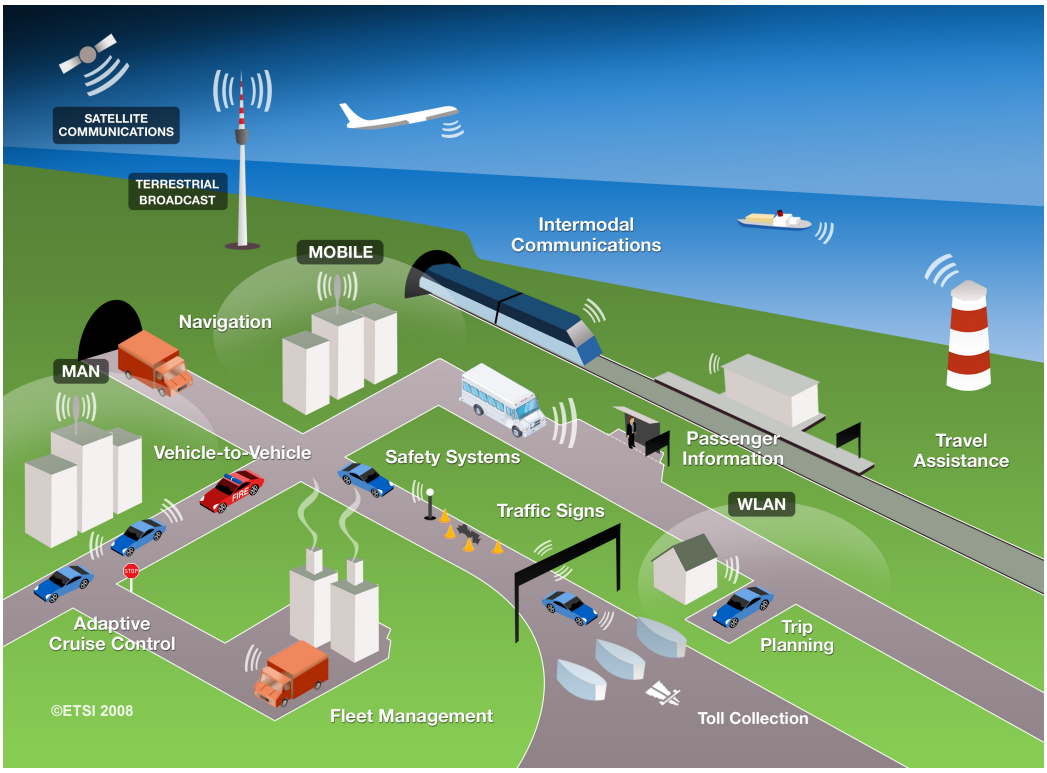


Figure 2.3: Future Intelligent Transport System [32]

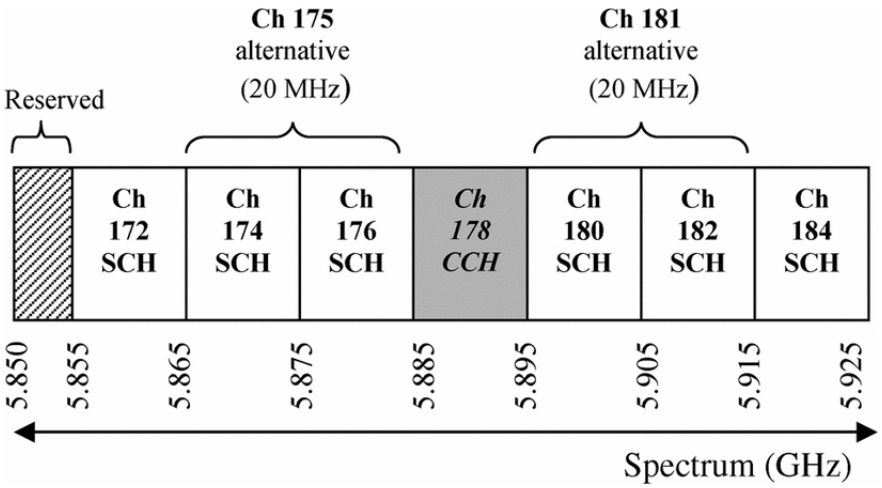


Figure 2.4: DSRC channel allocation [29]

---

nel, channel 178, is reserved for safety applications communications; all the others are classified as Service Channels and can be used by all types of applications, such as de-

picted in figure 2.4.

Other countries have also made similar efforts, for example, in Europe the spectrum between 5795-5815 MHz and between 5855-5875 MHz (and the following 20MHz are reserved for future needs) has been reserved for the vehicular communications; the 5855-5875MHz band has been reserved for the non-safety applications. Japan has already reserved the band between 5770-5850MHz.

2.6.2 IEEE 802.11p / WAVE

To address the characteristics and needs of VANETs, IEEE has made efforts to create a new set of rules, the WAVE standards, specially developed for vehicular networks. These standards are composed by: IEEE 802.11p and IEEE 1609.X. The IEEE 802.11p [17] focuses on lower layers (Physical Layer (PHY) and MAC), while the IEEE 1609.X [18] deals with the MAC layer and the higher layers.

As can be seen in Figure 2.5, the WAVE standards support two protocol stacks: the traditional Internet Protocol version 6 (IPv6) and WAVE Short Message Protocol (WSMP), developed specifically for this technologies. The reason for the existence of these two protocol stacks is to provide the capacity to accommodate messages with high priority and high latencies constraints (safety messages) as well as common messages to other networks

The IEEE 802.11p was created by modifying the IEEE 802.11a in order to obtain operations with reduced overhead in the DSRC band. The IEEE 802.11p, according to Jiang and Delgrossi [25], aims to:

- Perform the functions and services required by WAVE stations in an environment which rapidly changes and exchanges messages without requiring the association to a Basic Service Set (BSS).

- Define the WAVE signaling techniques and interface functions that are controlled by the IEEE 802.11 MAC.

Also according to Jiang and Delgrossi [25], three main changes were made, besides the change of the frequency from 5 GHz to 5.9 GHz of the PHY layer of IEEE 802.11a, in order to make it more suited to the needs of the vehicular communications. These changes were:

- 10 MHz channels, because with 20 MHz channels the guard time may not be enough to inter-symbols interference. Cheng et al. [7] have performed a study with different

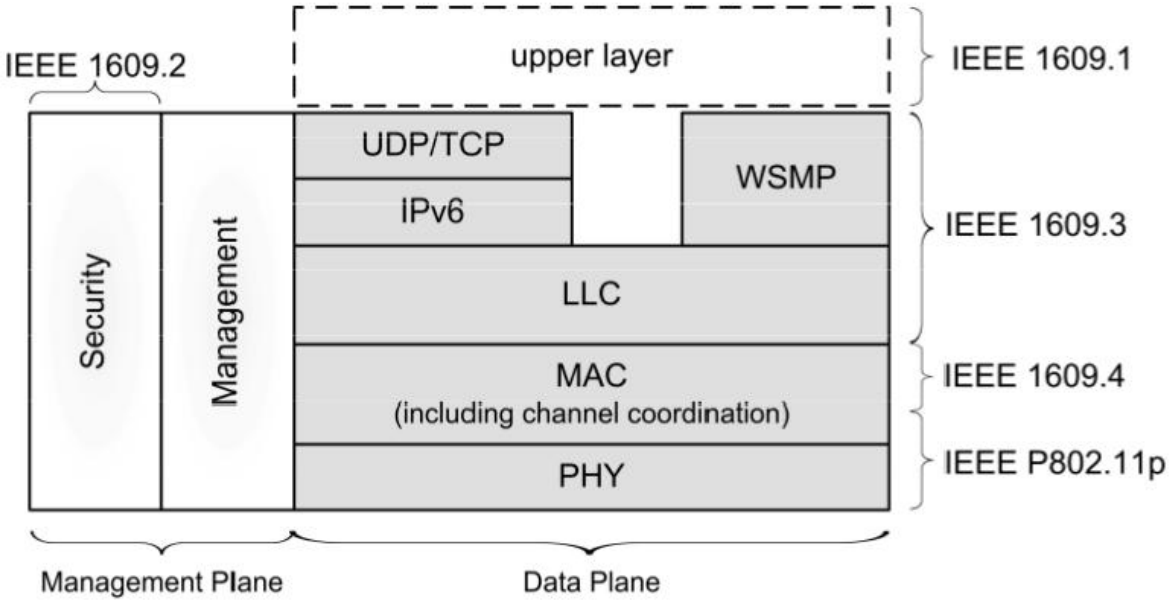


Figure 2.5: WAVE Protocol Stack [12]

---

frequencies and they concluded that the correct choice is to have channels with 10 MHz.

- Requirements in improved receiver performance, especially in rejection of adjacent channels.

- Improved transmission mask, this is more stringent than that required by IEEE 802.11a.

After defining the standard various studies on its performance were made. We will now resume the main conclusions and results.

Wang et al. [46] used the Network Simulator 2 (NS-2) [13] to study the behavior of MAC layer focusing on V2I communications. They concluded that, using a windows system of fixed size, as described in the standard, throughput problems due to the dynamics of vehicular networks may appear. To solve this problem, they presented two algorithms (a centralized algorithm and a distributed algorithm) to improve the protocol and increase throughput. The centralized algorithm assumes that the RSUs know the number of vehicles for which they want to transmit, and calculates the ideal probability of transmission in order to increase throughput. On the distributed algorithm, each vehicle requires the

local information and calculates the back off time depending on the channel conditions. Simulations with the two algorithms have shown significant improvements while using the IEEE 802.11p standard.

Eichler [14] conducted a study on the performance of the standard, concluding that, in scenarios with a high density of vehicles, mainly due to the problem mentioned above and accentuated by the fact that there is a constant exchange between SCH and CCH, it can lead to posts of security which are not delivered in useful time. It was proposed the use of a mechanism similar to the one proposed by Kosch et al. [30], in order to reduce the number of high priority messages to prevent long queues. This mechanism is based on assigning relevance to messages: the relevance of a message is calculated by estimating the benefit that the receiver node will have. Stibor et al. [42] evaluated the potential number of nodes and the maximum communication time between them, using a freeway as scenario, and concluded that the number of vehicle neighbors is an important input parameter for the algorithms responsible for choosing the next transmitter in a multi-hop communication scenario.

Alasmary and Zhuang [2] analyze the impact of the mobility on the performance of the MAC layer in a scenario without infrastructure, concluding that the relative velocity between the nodes has a great impact on the channel access by the MAC layer. This study proposed two dynamic priority systems to reduce contention and improve Packet Delivery Ratio (PDR), Simulations using NS-2 showed an improvement at the level of the PDR and on the average number of retransmissions per packet. An evaluation of the IEEE 802.11p communications potential was performed by Neves et al. [40], where a study on the scope of communication in real scenario was performed, concluding that it can get up to communication distances of more than 1 km if the vehicles are in line of sight, and about 100 m if the vehicles are in non-line of sight.

2.6.3 Multi-Technology approach

The deployment of the vehicular networks may be a slow process due the need of current vehicles adaptation by the owners who want them, or by including the communication systems (OBUs) directly by the automotive companies on their new vehicles, and the need to build the fixed infrastructures (RSUs). A way of accelerating this process is to use multi-technology systems. On other words, the systems should be able to connect to the fixed infrastructure, the RSUs, by WAVE technology, but they should also be able to connect to the currently existing WI-FI networks as well as the cellular network. The advantages of one or another should be measured in order to reduce the cost for the user without

damaging the system correct operation.

WI-FI networks are presently spread all over the cities, and some operators, such as ZON/FON, allow external users to access Internet using private routers of common subscribers through a reserved bandwidth. However that is not a cost free access unless the users are a subscriber of the same operator. On other hand, some cities (not all) share a WI-FI free connection for their habitants. The main problem is that the WI-FI technology has a relatively small range and is mostly concentrated within the main zone of the cities. Therefore, they are not a possible choice when on the highway or on any outside city scenario.

Nowadays, cellular networks cover almost every country and should be a good alternative when the vehicles are not in range of any RSU. With the introduction of high speed technologies such as HSDPA and LTE, which already cover a considerable area, they may satisfy the currently needs of bandwidth. However, cellular networks have a high latency value and usually represent high costs for the users.

The ideal scenario, until the majority of the vehicles are equipped with the OBUs and the RSUs are deployed on the main roads, is to use systems that, when on the inexistence of WAVE access points, use the available WI-FI access points, due to its lower costs and link latency, and only on last resort use a cellular connection.

This Dissertation will consider this scenario.

2.7 Routing and Dissemination

The vehicular ad-hoc networks differ from conventional wireless networks, not only because they experience rapid changes in wireless links, but also because they have to deal with different types of vehicles densities which form the network [27]. For example, vehicular networks on highways and in urban areas are more likely to form networks with high densities of vehicles during rush hours. Moreover, in rural areas, where the population is reduced, the vehicular networks tend to be formed from a low density of vehicles, experiencing often network fragmentation situations due to the small number of vehicles. Also, urban and highway scenarios experience situations of network fragmentation overnight.

Furthermore, it is expected that vehicular networks deal with a wide range of applications from security to leisure. Thus, the routing and dissemination algorithms should be efficient and should adapt to the characteristics of vehicular networks and applications, allowing different transmission priorities according to the type of application (whether or not a security related communication). Much of the research in terms of vehicular net-

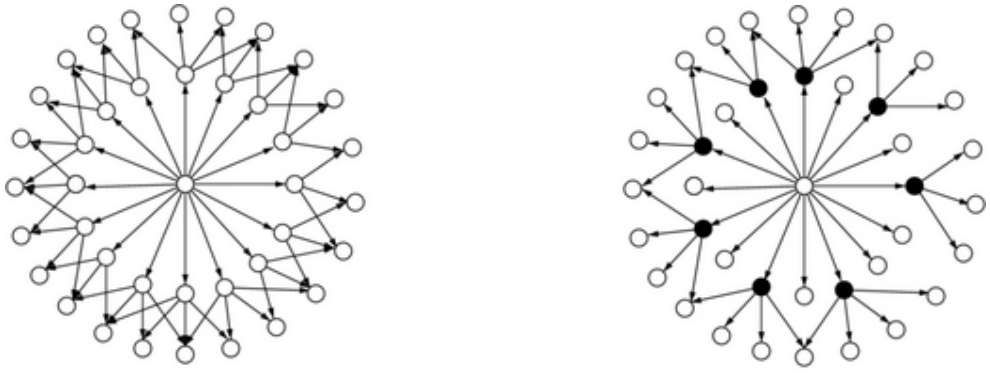
works was focused on analyzing routing algorithms, assuming that vehicular networks are well connected by nature. Until now, the penetration of the vehicular networks is somewhat low, which leads to the requirement of the existence of infrastructure support for a large-scale deployment that may cause retransmission of packets whenever there is a lower density of vehicles. Therefore, it is expected that, in the future, these networks have a greater penetration with a smaller number of infrastructure support.

With respect to the dissemination of messages, the spreading algorithms should depend on the density of the network and the type of application. For example, the dissemination of messages for applications related to security type must be broadcasted to ensure that the message is propagated to the desired cluster vehicle. In non-safety applications, the message must be transmitted in unicast or multicast because this type of transmission is most appropriate to the service itself.

We will now introduce the main routing protocols that may be applied on the VANETs.

2.7.1 OLSR

OLSR [10] was an initial attempt at standardizing a proactive link-state routing protocol. It is currently the most used ad-hoc routing protocol. According to [23], OLSR minimizes the overhead from flooding of control traffic by using only selected nodes, called Multi-Point Relays (MPRs), to retransmit control messages. This technique significantly reduces the number of retransmissions required to flood a message to all nodes in the network. Secondly, OLSR requires only partial link state to be flooded in order to provide shortest path routes. The minimal set of link state information required is that all nodes selected as MPRs declare the links to their MPR selectors.



(a) Pure flooding (b) MPR flooding

Figure 2.6: OLSR MPRs operation

2.7.2 Better Approach To Mobile Adhoc Networking (BATMAN)

BATMAN [39] is a different approach to routing. It builds routing tables, hence it is a proactive routing protocol; however, routes are acquired in a biologically inspired manner. This protocol is fundamentally different from classic link state and distance vector routing. It does not try to discover or calculate routing paths; instead, it tries to detect which neighbor offers the best path to each originator. The routing information is not communicated directly; instead, each node broadcasts packets called Originator Messages (OGMs) every second. When received by neighboring nodes, OGMs get re-broadcasted. Route selection for a given destination is based on the node from which the most OGMs have been received for a particular destination. The number of OGMs that can be accepted is limited to a constantly moving window. This window limits the history of OGMs that are allowed to describe a given route. The scalability of BATMAN counts on packet loss and thus, like other algorithms, OGMs are broadcasted as unreliable UDP packets. As nodes continuously broadcast OGMs, without packet loss, these messages would overwhelm the network. Therefore, it is unable to operate in reliable wired networks.

2.7.3 BABEL

Babel [9] is a proactive distance vector routing protocol. It was originally designed for wireless ad-hoc networks. Because of that, Babel is robust in the presence of mobility: only under very exceptional situations circumstances will it cause a transient routing loop, this is unlike OLSR, which will cause transient routing loops just after a mobility event before the new topology information is flooded throughout the network, BABEL protocol enjoys fairly fast convergence, since it uses triggered updates and explicit requests for routing information, and it usually converges almost immediately after the link quality measure has completed. This initial solution is not optimal: after converging to a merely satisfactory set of routes, it will take some time before optimizing the routing tables. Its updates are transmitted unreliably using IPv6.

2.7.4 Density-Aware Zone-based packet forwarding in vehicular networks (DAZL)

DAZL was specially created for the VANETs, according to [33], it is a forwarding protocol that combines three concepts in a novel way. First, multiple nodes cooperate in packet forwarding. Compared with traditional single relay schemes, this provides robustness against changes in topology and packet delivery rates. Second, network-layer slotting

is used to control duplication and contention in high density scenarios. Third, a distributed prioritization algorithm is used to opportunistically maximize hop length. On the tests performed, DAZL has provided improvements of up to 60% in throughput over single relay forwarding, while ensuring low latency and replication.

2.7.5 Comparing the routing protocols

These routing protocols, except the DAZL, were tested in a previous MSc Dissertation [11], and it was concluded that BABEL is the most suitable protocol for the use on VANETs. It was verified that the OLSR should not be used in these networks, because it takes some tens of seconds to detect changes in the network topology, which is unaffordable in vehicular networks due its high mobility. In terms of response to the mobility of vehicles between the available RSUs, it was verified that the protocols BATMAN and Babel can only adapt to this scenario if the speed of the mobile nodes is reduced, for example, for speeds of 50 km/h and 70 Km/h, it was already obtained high link loss times. Again, in this test the OLSR protocol performance was much lower than the other protocols confirming that this protocol is not applicable to VANETs.

As DAZL was designed to be applied on the vehicular networks, it is then expected that its performance is better. However, there are not enough studies yet.

2.8 VANETs Applications

VANETS are considered as one of the most prominent technologies for improving the efficiency and safety of modern transportation systems. For example, vehicles can communicate detour, traffic accident, and congestion information with nearby vehicles early to reduce traffic jam near the affected areas. VANET applications enable vehicles to connect to the Internet to obtain real-time news, traffic, and weather reports, and they also fuel the vast opportunities in online vehicle entertainments, such as gaming and file sharing via the Internet or the local ad-hoc networks.

Applications such as safety messaging are near-space applications, where vehicles in close proximity, typically in the order of few dozen meters, exchange status information to increase safety awareness. The aim is to enhance safety by alerting of emergency conditions. Applications for VANETs are mainly oriented to safety issues (e.g., traffic services, alarm and warning messaging, audio / video streaming and generalized infotainment), in order to improve the quality of transportation through time-critical safety and traffic management applications [21], two examples can be seen in figures 2.7 and 2.8. At the same time, also

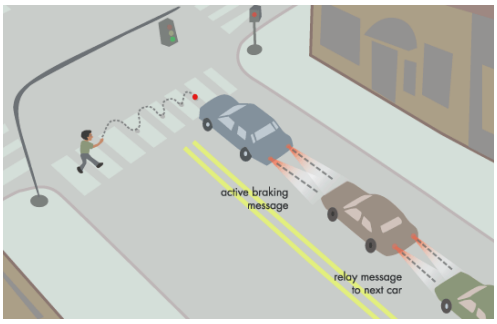


Figure 2.7: Emergency Braking Message

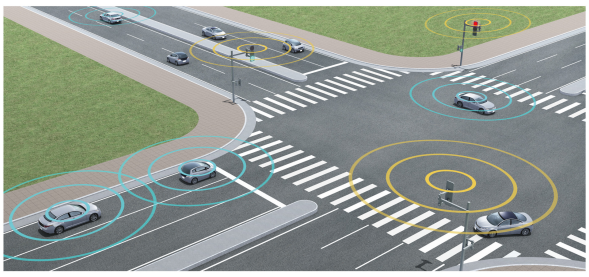


Figure 2.8: Traffic Lights Applications

entertainment applications are increasing (e.g., video streaming and video-on-demand, the interest on web browsing and Internet access to passengers to enjoy the trip).

Applications of alarm messaging have strict latency constraints of the order of few milliseconds, and very high reliability requirements [34]. In contrast, applications such as traffic and congestion monitoring require collecting information from vehicles that span multiple kilometers [15]. The latency requirements for data delivery are relatively relaxed i.e., they are delay-tolerant; however, the physical scope of data exchange is much larger. In contrast, general purpose Internet access requires connectivity to the backbone network via infrastructure, such as Road-Side Units (RSUs).

Non-safety applications are expected to create new commercial opportunities by increasing market penetration of the technology and making it more cost effective. Moreover, comfort and infotainment applications aim to provide road travelers with needed information support and entertainment to make the journey more pleasant. They are very diversified and ranges from traditional IP-based applications (e.g., media streaming, voice over IP, web browsing, etc.) to applications unique to the vehicular environment (e.g., point of interest advertisements, maps download, parking payments, automatic tolling services, etc.).

2.9 Mobility

In traditional IP routing, IP addresses represent a topology. Routing mechanisms rely on the assumption that each network node will always have the same point of attachment to the Internet, and that each node's IP address identifies the network link where it is connected. In this routing scheme, if we disconnect a mobile device from the Internet and want to reconnect through a different network, we have to configure the device with a new IP address, and the appropriate network mask and default router. Otherwise, routing

protocols have no means of delivering datagrams (packets), because the device's network address does not contain the necessary information about the node's network point of attachment to the Internet.

Vehicles may acquire information and services through V2V or V2I communications. The V2V communication is based on the DSRC technology, while the V2I communication is based on DSRC, GPRS/3G/LTE, WI-FI or WiMAX. Since the moving speed of the vehicles in the VANET is so high, it is harder to maintain a seamless handoff and a stable connectivity to the Internet. To achieve seamless handover for IP based communications, the IP of the mobile device must be assigned and reassigned efficiently. Mobile Internet Protocol version 4 (MIPv4) [6] has been proposed by the IETF. Since MIPv4 may face problems like the short of IP addresses, and poor security and Quality of Service (QoS), MIPv6 [26] is proposed by IETF.

The Proxy Mobile IPv6 (PMIPv6) [17] is a network based mobility management protocol standard that was ratified by the Network-based Localized Mobility Management (NetLMM) working group [28] of the IETF. PMIPv6 is a protocol that uses the same concepts as used in MIPv6, but modified to operate in the network part only instead of involving the Mobile Node (MN) as well. PMIPv6 is claimed to possess a number of advantages over the host based mobility management protocols in use today. The main advantage of using PMIPv6 is the freeing up of the MN in doing any mobility related activities and thereby saving its resources. The saving of resources may result in its usage for other purposes, or even enable otherwise capabilities restricted devices to operate in the PMIPv6 domains. Other advantages include reduced signaling traffic volume and no tunneled packets in the access network.

Network mobility stands for the mobility support of an entire network which moves together between different access points, it has attracted large attention to provide vehicles such as trains with Internet connectivity [16]. However network mobility protocols such as NEMO are MIPv6 based which means that it has host based mobility, an unwanted situation. Hybrid implementations like PNEMO (PMIPv6-based NEMO) or FPNEMO (Fast PNEMO) try to join the advantages of mobility protocol NEMO with the ones of the PMIPv6 in order to support network mobility without the need of involving the host [43] [31]. Another proposed implementation is the N-PMIPv6 (Network - PMIPv6) which intends to modify the PMIPv6, keeping its advantages, but now providing support for network mobility [24].

According to Zhu et al. [49], the chosen mobility protocol for a vehicular network environment should include the following characteristics:

- `Mobility without packet loss`: VANETs should be an extension of the Internet, and the vehicle mobility should be transparent, which means that, independently of the technology used by the vehicle to connect to the Internet, it should always be able to maintain its Internet Gateway available and stable.

- `Smooth and fast handover`: Due to the high mobility characteristic of the vehicle networks, it will be recurrent the need of performing handover between access points of the same wireless technology, horizontal handover, or between different technologies, vertical handover. It is then required that this process be very fast and smooth due the possible high velocity of each vehicles changing access points.

- `IPv6 support`: In order to maintain connection, it is needed a permanent IP address for each vehicle, and IPv6 will make this support much easily.

- `Efficiency and scalability`: VANET networks have propensity to accommodate thousands of vehicles, which makes the need of a highly scalable and efficient mobility protocol a priority.

The next sub-sections will summarize the characteristics of the referred mobility protocols.

2.9.1 MIPv6

MIPv6 is a protocol developed as a subset of Internet Protocol version 6 (IPv6) to support mobile connections. MIPv6 is different from the IETF Mobile IP standard [5], and it is designed to authenticate and move mobile devices (known as mobile nodes) using IPv6 addresses. MIPv6 allows a mobile node to transparently maintain connections while moving from one subnet to another. Each device is identified by its home address, although it may be connecting to it through another network. When connecting through a foreign network, a mobile device sends its location information to a home agent, which intercepts packets intended for the device and tunnels them to the current location. MIPv6 uses IPv6 routing header rather than IP encapsulation (as on MIPv4), and therefore, it naturally supports Route Optimization. All new messages used in MIPv6 are defined as IPv6 Destination Options.

The MIPv6 protocol uses a specific terminology for the various entities as well as for the new messages introduced by it. Their description will now be exposed.

Terminology

The following definitions are important for understanding the basics of Mobile IP and will be used throughout the description of this protocol and some of its variants.

- `Mobile Node (MN)`: an IP device capable of changing its attachment point to the Internet while maintain higher layer connectivity through mobility functionality.
- `Care-of Address (CoA)`: IP address of MN at its current Internet attachment point.
- `Correspondent Node (CN)`: an IP device that is communicating with Mobile Network Node via IP protocol.
- `Home Agent (HA)`: host on the Home Network that enables the MN to roam.
- `Home Network (HN)`: network that a MN belongs to when it is not roaming, i.e., the network that is associated with the network link of the Home Agent.
- `Foreign Network (FN)`: network where the MN is operating when away from its HN.
- `Home Address`: MN's IPv6 address (assigned when connected to its home network) that remains unchanged even if it changes its attachment point.
- `Binding`: the association of the MN's home address with a CoA for a certain period of time. That is, between the stable home address and the MN's current location.
- `Binding cache (BC)`: a cache stored in volatile memory containing a number of bindings for one or more mobile nodes. A BC is maintained by both the CN and the HA. Each entry in the BC contains the MN's home address, CoA, and the lifetime that indicates the validity of the entry [26].
- `Router Solicitation (RS)`: a Router Solicitation message may be issued by a host to cause local routers to transmit information, a Router Advertisement, from which it can obtain information about local routing or perform stateless auto-configuration [37].
- `Router Advertisement (RA)`: a Router Advertisement message is issued periodically by a router or in response to a RS message from a host [37].
- `Binding Update (BU)`: the purpose of this message is to inform the HA of the MN's current address (i.e., CoA) [26].

- `Binding Acknowledgment (BA)`: the HA, after receive the BU and make an association between the home address to the MN and the CoA it received, responds with a binding acknowledgment [26].

Operation method

The operation of MIPv6 is based on three basic mechanisms:

- `Discovery`: Mobility Agents (FN) announce their availability by sending Internet Control Message Protocol (ICMP) RA messages. The Mobile Node can immediately require it by sending an ICMP RS message.

- `Registration`: When a MN enters a FN, and after obtaining a CoA, it sends a BU to its HA with the information obtained from the new CoA; HA stores this information in its BC in order to know where to forward the packets destined to the MN. A MN can register multiple CoAs if it can bind to more than one FN simultaneously.

- `Tunneling`: When the HA receives the BU message, it sends a message BA to MN, to confirm the registration. Then it creates a tunnel to the respective CoA, forwarding by this tunnel all packets destined to the MN.

MIPv6 also provides a mechanism called Return Routability that allows CNs with IPv6 support to directly communicate with MNs. The Return Routability process occurs as follows:

- Two messages are sent: a Home Test Init (Hoti) message that is sent to the CN via HA and Care-of Test Init (Coti) message which is sent directly to the CN.

- These messages aim to obtain a home keygen token and care-of keygen token which are sent via Home Test (HoT) and Care-Test (CoT), respectively.

- Then, the MN sends a BU message to the CN to update its BC.

- At last, the CN sends a BA to the MN indicating that the update was accepted.

When a CN wants to send a message, it checks in its BC if it has any input to the destination of the packet. If it finds it, the packet is sent directly to the CoA, thus avoiding the traversal through the HA which will end up on an improvement in the delivery time of the packet, and since there is no need to encapsulate the package, it also reduces the

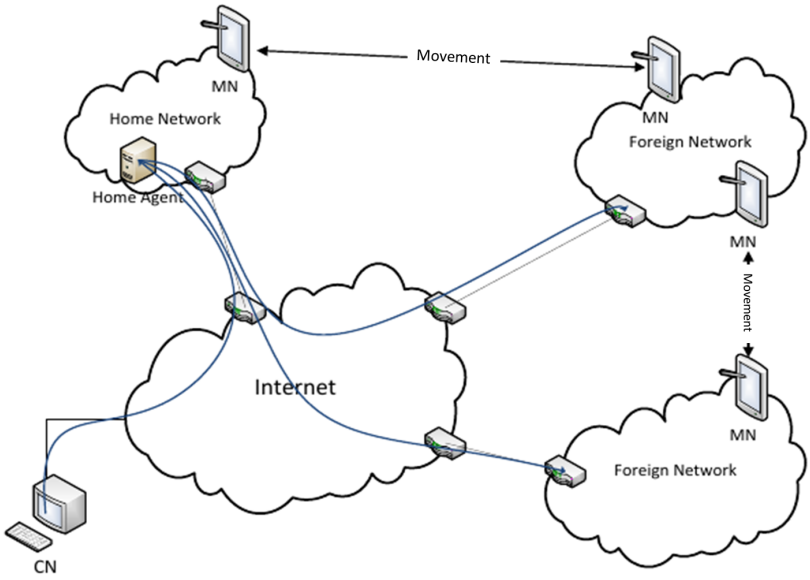


Figure 2.9: MIPv6 Arquitecture [11]

overhead introduced in the network. If there is no entry is found, the packet is routed normally to the HA and then sent through the tunnel to the CoA.

Although this protocol satisfies the mobility of a node, it does not support the mobility of a complete network, thereby not satisfying the need of VANETs in moving parts of the network along the various access points, for example, the users inside a car move along with it. On the other hand, this protocol requires interaction by all mobile nodes, which is not acceptable because it is intended to allow any device to connect to the network broadcasted by the vehicle, such as a simple mobile phone. This protocol would require that all mobile nodes have specific software running to connect to the network. Therefore, it is not a protocol suitable for use in VANETs.

2.9.2 PMIPv6

PMIPv6 is one of the proposed solutions to support a localized mobility management for a MN [45].

Terminology

The following definitions are important for understanding the basics of PMIPv6, and will be used throughout the description of this protocol and some of its variants.

- `Local Mobility Domain (LMD)`: Network that is PMIP-enabled. The LMD contains one Local Mobility Anchor and multiple Mobile Access Gateways.
- `Local Mobility Anchor (LMA)`: All traffic from and to the mobile node is routed through the LMA. The LMA maintains a set of routes for each MN connected to the LMD.
- `Mobile Access Gateway (MAG)`: The MAG performs the mobility related signaling on behalf of the MNs attached to its access links. The MAG is usually the access router (first hop router) for the MN.
- `NetLMM`: Network based Localized Mobility Management (IETF working group for network-based mobility support).
- `Binding Cache (BC)`: Cache maintained by the LMA that contains BCEs.
- `Binding Cache Entry (BCE)`: Entry in the LMA BC. An entry has the fields MN-ID, MAG proxy-CoA and MN-prefix.
- `Binding Update List (BUL)`: Cache maintained by the MAG that contains information about the attached MNs.
- `Proxy Binding Update (PBU)`: PMIP signaling packet sent by the MAG to the LMA to indicate a new MN. The PBU has the fields MN-ID (e.g. MN MAC), MAG address (proxy-CoA) and handoff indicator to signal if the MN-attachment is a new one or a handoff from another MAG.
- `Proxy Binding Acknowledge (PBA)`: Response to a PBU sent by the LMA to the MAG. The PBA contains the MN-ID, the MAG address and the prefix assigned to the MN.
- `Proxy care of address (proxy-CoA)`: IP address of public interface of MAG. The proxy-CoA is the tunnel endpoint address on theMAG. The LMA encapsulates packets destined to the MN into a tunnel packet with destination address = Proxy-CoA.
- `Mobile Node Identifier (MN-ID)`: Unique identifier of mobile node, e.g. one of its MAC addresses.
- `Home Network Prefix (MN-HNP)`: Prefix assigned to the MN by the LMA.

Operation method

PMIPv6 is designed to provide network-based mobility management support to an MN in a topologically localized domain. Figure 2.10 represents the operation method of the PMIPv6 protocol.

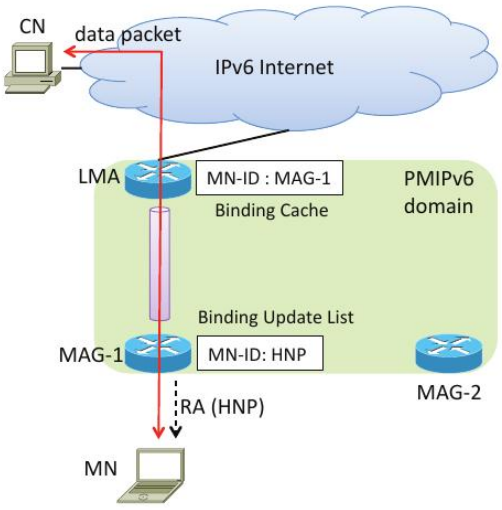


Figure 2.10: PMIPv6 Arquitecture [43]

According to [43], the handover procedure works as follows:

- When an MN enters into a new PMIPv6 domain, initially it attaches to MAG-1 in the domain. Then the access authentication procedure is performed using an MN-ID via the deployed access security protocols on the access network. After successful access authentication, the MAG-1 obtains the MN's profile, which contains the MN-Identifier, LMA address and supported address configuration mode.
- To update the LMA about the current location of the MN, MAG-1 sends a PBU message to the LMA on behalf of the MN. Upon receiving the PBU message, the LMA assigns a MN-HNP and creates a BCE that binds the MN-HNP to a Proxy-CoA, which is the address of MAG-1. The LMA sends a PBA message including the MN-HNP.
- Upon receiving the PBA message, MAG-1 sets up a tunnel to the LMA and adds a default route over the tunnel to the LMA. It also creates a BUL. The MAG-1 then sends RA messages to the MN on the access link to advertise the MN-HNP as the hosted on-link-prefix.

- When the MN receives these RA messages, the MN configures the IP address using either a state full or stateless address configuration modes. After successfully completing the address configuration procedure, the MN uses this address for packet delivery.

From now on, the LMA can route all the traffic directed to the MN through the established route. When the MN changes its point of attachment, i.e., requires connection to another MAG, the following handover procedures start:

- When the MN moves to the access network of MAG-2, MAG1 receives a LGD (*Link Going Down*) trigger and detects that the MN has moved away from its access link. Therefore, MAG-1 sends a DeReg PBU (De-Registration PBU) message to the LMA with the lifetime value set to zero for de-registration.

- Upon receiving the PBU message with a zero lifetime value, the LMA sends a PBA message to MAG-1 and waits for a minimum delay before it deletes the MN BCE.

- When MAG-2 detects the attachment of MN, MAG-2 obtains the MN profile using an MN-ID after successful access authentication. Then, the registration follows as was explained before.

This protocol solves a major problem of the MIPv6 protocol: it eliminates the need for interaction by the mobile nodes allowing any common device to connect to the network via an access point. However, this protocol, such as MIPv6, only allows the nodes to connect to the fixed access points, i.e. it allows linking the mobile nodes to a MAG/RSU, providing no mobility to a complete network. So this is not an ideal protocol for VANETs if we aim to support complete network mobility.

2.9.3 NEMO

NEMO (NEtwork MObility) is an extension of Mobile IP that enables an entire network to change its attachment point to the Internet.

Terminology

In order to introduce the NEMO protocol, it is needed to add the following terms to the ones already introduced on the MIPv6:

- `Mobile Router (MR)`: A router capable of changing its point of attachment to the Internet without disrupting higher layer connections of attached devices.

- `Access Router (AR)`: Router that provides Internet access to a MR.
- `Mobility Agent (MA)`: Any IP device, including MR and HA, that performs mobility functions.
- `Mobile Network Node (MNN)`: Any IP device on a mobile network. Mobile Network Nodes may be fixed to the mobile network (LFN - Local Fixed Node), or visiting the mobile network as mobile nodes (VMN - Visiting Mobile Node).

Operation method

Under NEMO, a MR takes over the role of the MN in performing mobility functions. Nodes that are attached to a MR, MNNs, are not aware of the network's mobility and do not perform any mobility functions. MRs also sends BUs to their HAs. However, BUs from MRs also contain the mobile network's network prefix. HAs will bind an entire network prefix to the MR's CoA and forward all packets for that network to the MR. Figure 2.11 represents the operation method of the NEMO protocol.

When the MR moves away from the home link and attaches to a new access router, it acquires a CoA from the visited link. The MR can at any time act either as a Mobile Host or as a MR. It acts as a Mobile Host for sessions it originates and provides connectivity to the Mobile Network. As soon as the MR acquires a CoA, it sends a BU to its HA. When the HA receives this BU, it creates a cache entry binding the MR's Home Address to its CoA at the current point of attachment.

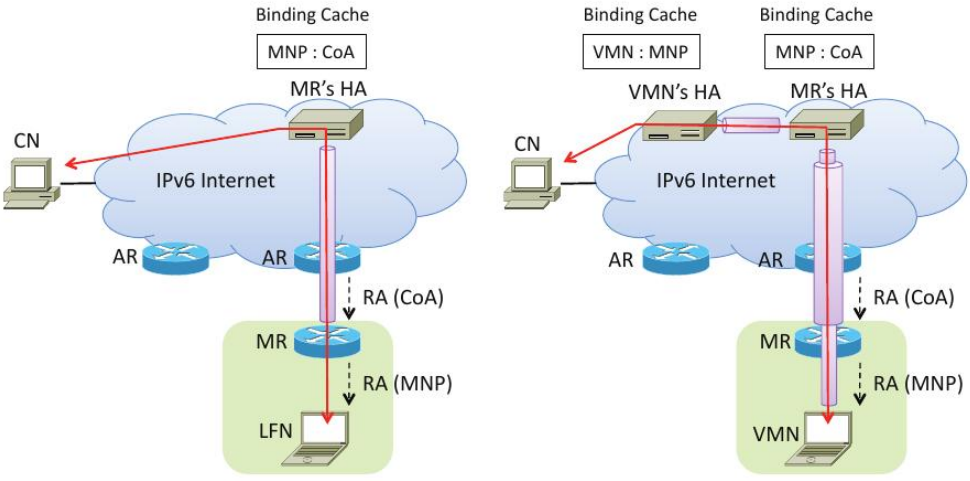


Figure 2.11: NEMO Arquitecture [43]

The NEMO extends the functions of Mobile IPv6 to support the mobility of complete networks eliminating its main disadvantages. However, it is not a very efficient protocol. As have been shown [43], PNEMO and PMIPv6 show better results on both registration time and processing time than NEMO. Therefore, they should be more suitable for a highly dynamic network such as the VANETs.

2.9.4 PNEMO

PNEMO (PMIPv6-based NEMO) employs network-based localized mobility management to avoid signaling message loss on wireless link during handover. PNEMO components are similar to the ones on PMIPv6 and it also employs the home network prefix and the mobile network prefix as defined in PMIPv6 [43].

Operation method

PNEMO employs only a single tunnel between the LMA and the MAG to avoid multiple tunneling if a mobile network is nested, and to achieve this, it introduces the NEMO State Table (NST) in the MR. The NST is composed by the NSTEs (NEMO state table entries), each of which manages the subMR or the Visited Mobile Node (VMN) under the MR. The NSTE is composed by the node ID field and the upper router ID field. The node ID field contains the ID of the subMR or the VMN under the MR. The upper router ID field contains the identifier of the upper level router to which the node of this entry is connected. In network-based localized mobility management, the MAG can obtain only the identity of the MR or the VMN that attaches to the MAG, i.e., the MAG cannot obtain the information of the VMN or the nested mobile network under the MR when the MR executes handover. To solve this, PNEMO extends the BCE in the LMA and the binding update list entry (BULE) in the MAG, so that the LMA and MAG can manage the VMN or the nested mobile network. To register the information of the VMN or the nested mobile network with the BCE and the BULE, PNEMO defines four control messages:

- The Nested Binding Update (NBU) message;
- The Nested Binding Acknowledgment (NBA) message;
- The Proxy Nested Binding Update (PNBU) message;
- The Proxy Nested Binding Acknowledgment (PNBA) message;

The NBU and the NBA messages are exchanged between the sub-MR and the upper level MR (or the sub-MR) to inform the upper level MR of the information of the lower level sub-MR and the VMN connected to the lower level sub-MR. When the MR (or the sub-MR) receives the NBU message from the lower level sub-MR, the MR creates the NSTEs of the lower level sub-MR and the VMNs included in the NBU message. All this process can be identified on the figure 2.12.

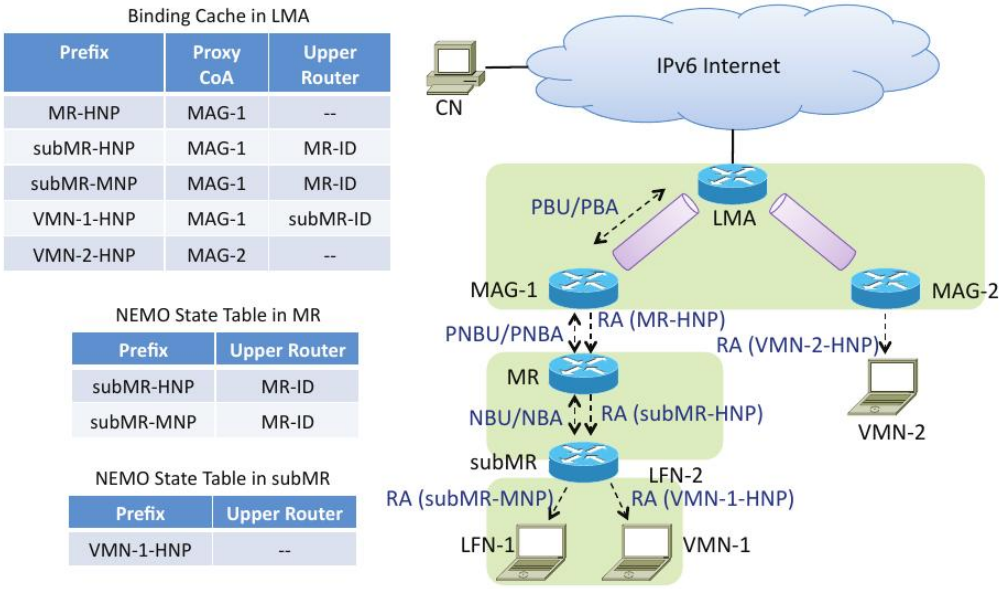


Figure 2.12: PNEMO Arquitecture [43]

PNEMO supports either host and network mobility, and has been shown that it has a reduced registration and processing time, which makes this a suitable protocol to be applied on VANETs. However, this has a particularity of work on a hierarchical manner, on other words, when a node moves from one access point to another, all routers between it and the central point (LMA) need to be updated, and that can increase the handover time in the case of highly nested networks. A different approach was taken by N-PMIPv6, which will now be introduced.

2.9.5 N-PMIPv6

N-PMIPv6 extends PMIPv6 to support network mobility. It introduces the mobile MAG (mMAG) in addition to the LMA and the MAG (fixed MAG). Figure 2.13 depicts the operation of the protocol.

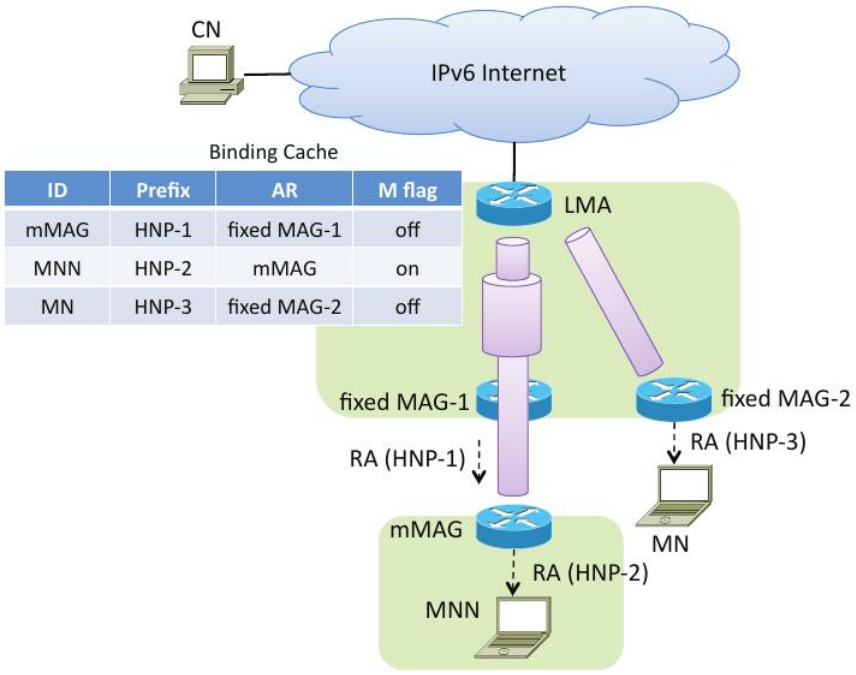


Figure 2.13: N-PMIPv6 Arquitecture [43]

Operation method

According to [43] and [24], the registration and handover procedures are performed as follows:

- When a mMAG with a MNN attaches to the fixed MAG-1, the fixed MAG-1 sends the PBU message containing the mMAG-ID to the LMA.
- Upon receiving the PBU, the LMA assigns the mMAG the HNP-1 and creates the BCE. Next, the LMA returns the PBA to the fixed MAG-1.
- Upon receiving the PBA, the fixed MAG-1 sends the RA message containing the HNP-1 to the mMAG.
- Upon receiving the RA message, the mMAG sends the PBU message containing the MNN-ID to the LMA.
- Upon receiving the PBU message, the LMA assigns the MNN the HNP-2 and creates the BCE. N-PMIPv6 adds a new field, the M flag, to the BCE. The M flag of MNN BCE is set to indicate that the MNN is connected to a mobile network.

- Next, the LMA returns the PBA to the mMAG. Upon receiving the PBA, the mMAG sends the RA message containing HNP-2 to the MNN.

- The data packet destined to the MNN first reaches the LMA. The LMA finds MNN BCE. Since the M flag is "on" in the MNN BCE, the LMA searches for mMAG BCE. Next, the LMA encapsulates the packet for tunneling to the mMAG and encapsulates it again for tunneling to the fixed MAG. The LMA forwards the packet to the fixed MAG. The fixed MAG removes the outer tunneling header and forwards it to the mMAG. The mMAG retrieves the original packet and forwards it to the MNN.

- When the mMAG moves to the fixed MAG-2, the same procedures as in the initial registration are executed. In this procedure, the AR field of the mMAG BCE is updated from fixed MAG-1 to fixed MAG-2. Other fields of mMAG BCE and MNN BCE remain unchanged. Thus, in N-PMIPv6, the signaling messages are not sent on the wireless link when a handover occurs.

N-PMIPv6, as the PNEMO, supports either host and network mobility, but instead of following a hierarchical methodology, every router only has to keep record of every mobile nodes or routers connected directly; therefore a router which as a router connected to it does not have to know the mobile nodes that may be connected to that router. The only entity with information of the entire network is the LMA and the packets are forward through tunneling. However, it generates more overhead over the network due to the tunneling method. Even so, it is a suitable protocol to be applied to VANETs.

This was the protocol chosen to be implemented as part of this Dissertation due to its features which satisfy the VANETs needs, and also because it can be directly implemented from the PMIPv6, which has been previously submitted to real applications tests on our group in a previous MSc Dissertation [11].

2.10 Chapter Considerations

In the current chapter we described the main concepts required to understand the work developed along this Dissertation, which are the vehicular networks and the mobility protocols required to improve the users experience while connected to this type of networks.

With respect to vehicular networks, it is obvious the positive impact that they can take on today's society; for that reason many countries are already making efforts on the research and development of this type of networks. A new access technology, the IEEE 802.11p / WAVE, has been specially developed to support the unique characteristics of

these networks; however, there are just a few real studies containing this standard. It is imperative that the current existing protocols are evaluated and adapted to that new access technology. The integration of the VANETs with the already available networks is also important, since it will accelerate its deployment.

With respect to the mobility protocols, there are still few studies about this theme, and even fewer including their evaluation with the WAVE protocol. Since mobility is vital for providing an enjoyable experience for the users of the VANETs, it is important to evaluate the mobility protocols performance on a vehicular scenario in order to find one which could provide the required support.

After this introduction to the VANETs, the next chapter focuses on the specification and implementation of the mobility protocol for terminals and networks, and on the changes required on the mobility approach to make it work with the WAVE/DSRC technology, and in real environments of terminals and networks running IPv4.

Chapter 3

Mobility Protocols

3.1 Introduction

In order to allow users in vehicular networks to have Internet access and all the other entertainment and safety applications, the OBUs in the vehicles must be able to connect to the available IEEE 802.11p RSUs or any other connections available (free WI-FI access points or cellular networks) maintaining the sessions active, so that users do not experience any loss of connection. A mobility protocol associated with an efficient connection manager is then needed.

However, through an analyzis of vehicular networks unstable topology and highly dynamic behavior, we can concluded that a network mobility protocol is needed; when a car moves along the road, it takes all users that are inside the car so all this subnet must be supported by the mobility protocol. We consider that buses and cars shall be able to work as mobile gateways, connecting to each other and to the fixed infrastructure in order to extend the range of the network with the ability to access the Internet.

This Dissertation aims to develop a network mobility mechanism to support both vehicles and passengers mobility when connected to the vehicular networks. This mechanism will be evaluated in a real network in the various scenarios presented in section 3.2, for both IEEE 802.11p and IEEE 802.11g technologies. In order to achieve this network mobility support for VANETs, we will perform the following tasks:

- Implement a mobility mechanism based on N-PMIPv6.
- Integrate with a connection manager to automatize the selection and connection to the best available network.
- Integrate with the IPv4 network, both Internet and terminals.

- Adapt the mechanism to work properly with the IEEE 802.11p / WAVE technology.

The N-PMIPv6 was developed taking as basis the available PMIPv6 implementation, originally created by OAI and after modified in our group in a previous MSc Dissertation [11], in order to improve mobility of terminals with no packet loss. Our approach will consider two different wireless technologies, the IEEE 802.11g, usually known as WI-FI, one of the most common technologies nowadays, and with the IEEE 802.11p, a technology developed specially for vehicular networks and implemented also in our group [3]. Comparing how those technologies react to the handover process will allow us to evaluate their application in real vehicular environments. Our PMIPv6 approach is also able to deal with cellular networks and vertical handovers including cellular. Our N-PMIPv6 approach will keep this support, although it is not the focus of our scenarios in section 3.2.

The mobility protocols only act at the network layer; then, an external entity is needed to trigger the handover on the link layer. Therefore, a connection manager, capable of evaluating the available connections and trigger the handover to the best one, need also to be implemented. The connection manager implemented on this Dissertation chooses the connection accordingly to the signal RSSI: the one with higher RSSI is considered the best one. As a future work the connection manager could be significantly improved if it evaluates not only the signal RSSI, but also the speed and direction of the vehicle which will help prevent handovers to stations that are going to be farther from the car as long as it moves, if there are any stations ahead they will probably be a better choice. This should help reduce the number of performed handovers. This advanced connection manager has been performed in a parallel MSc Dissertation and will be integrated with this work.

In order to encourage the commercial support for the development of VANETs, it is important to have results that can already be shown to a regular user to prove its utility. Therefore, we will allow users within the vehicles to access the Internet like they usually do on their home or work place. But most of nowadays personal devices only support IPv4, which is not compatible with the mobility protocol developed. The requirements to overcome this problem will also be presented and developed.

This chapter is then divided as follows. Section 3.2 introduces the architecture to be studied as well as the interaction between the various entities involved in the mobility. Section 3.3 introduces the PMIPv6 protocol taking into account the various changes that it has been subjected to support optimistic handover in the framework of the previous MSc Dissertation [11]. This is the version of the protocol selected as basis for implementing the protocol N-PMIPv6. In section 3.4, it will be explained the problems detected due to incompatibilities of the mobility protocol and the WAVE technology on the experimental

tests and the solutions adopted. In Section 3.5, it will be detailed the implementation of the N-PMIPv6 network mobility protocol. Section 3.6 introduces the necessary modifications in order to allow the mobile MAG (mMAG) to share an IPv4 Internet connection to the users within the vehicle. In section 3.7, it will be introduced the connection manager and how it integrates with the mobility protocol. Finally, in section 3.8 we present the chapter considerations.

3.2 Scenarios and Architecture

Nowadays there is a wide variety of network access technologies available on several access points spread over the roads and buildings; when vehicles move around, they will often have to make handover between access points of the same technology, horizontal handover, or between access points of different technologies, vertical handover. A moving vehicle will take with it everyone who is connected to its private network, and therefore, it will be necessary not only to provide mobility to the vehicle, but also to all its users connected through the OBUs in each vehicle.

The following scenarios are the most important ones to be analyzed according to the purpose of this Dissertation. These scenarios will be described along with the roles of the mobility protocol and the connection manager.

The scenario in Figure 3.1 represents the most common handover scenario expected on vehicular networks, as the vehicle moves along, it will have to connect to the RSUs on the road, so it can continue to allow Internet access to the users connected to it. This assumes that the mobility protocol is able to address the network formed by the vehicle and all its dependents. This scenario intends to evaluate the horizontal handover between access points IEEE 802.11p with only one hop (one mMAG). This is expected to be completely transparent to the users of the vehicle network.

As the N-PMIPv6 provides network mobility support, it shall provide the support needed to move the network composed by the car and its dependents along the access points. On the other hand, the connection manager will scan the available access points and trigger the handover to the best available network. In this specific scenario, when the RSU2 offers a better connection than the RSU1, it will trigger the handover of the OBU present on the vehicle from the RSU1 to the RSU2.

The scenario in Figure 3.2 is similar to the previous one, but this case aims to evaluate the vertical handover technology from IEEE 802.11p to IEEE 802.11g or the opposite. Likewise, it is expected the handover process to be completely transparent to the users

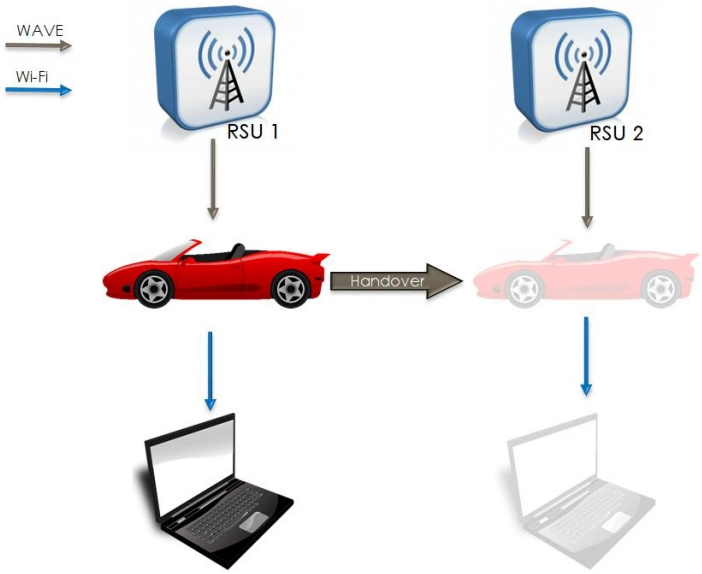


Figure 3.1: Horizontal network handover between RSUs using the IEEE 802.11p

within the vehicle. We will evaluate the metrics associated with the handover process between access points of different access technologies with only one mMAG (the bus).

In this scenario the mobility protocol, N-PMIPv6, shall provide the network the support needed to move the network composed by the bus and the users inside between the access points. The connection manager will be responsible to trigger the handover to the WI-FI access point when it offers a better connection than the RSU.

The scenario in Figure 3.3 represents the case where a user is connected to a vehicle, and at a given moment it leaves the vehicle (for example, in a bus stop), but aims to continue with his active sessions while connecting to an exterior access point, as an example, a WI-FI hotspot available on the near building. We will evaluate the link stability and the behavior of the terminal during the handover process, such as the time of disconnection, in a real Internet using case.

In this scenario the N-PMIPv6 protocol shall support the movement of the user between the access point within the bus and the one outside it, maintaining the users active sessions. The connection manager has no interaction on this point, since it should be the user of the personal device to select the new connection point, this process can be automated if the personal device has the needed software which shall act similar to the connection manager.

The following scenario, Figure 3.4, is a relevant case of study to this type of networks, as it is required to allow handover to networks at different hops away (number of mMAGs

Figure 3.2: Vertical network handover between RSU and Access Point

Figure 3.3: Horizontal handover between Access Points at different number of hops

---

that the link crosses). This scenario will evaluate the handover to a mMAG on a higher level of hops (two in this example) and then the opposite. Providing the protocol the ability to handle multi-hop handovers will allow, for example, extending the network range seamlessly.

In this scenario the mobility protocol shall provide the support needed to move the network composed by the car and its users from a mMAG, the bus, to another mMAG, the car, and therefore performing handover between two chained MAGs. The connection manager will be responsible to trigger the handover between them.

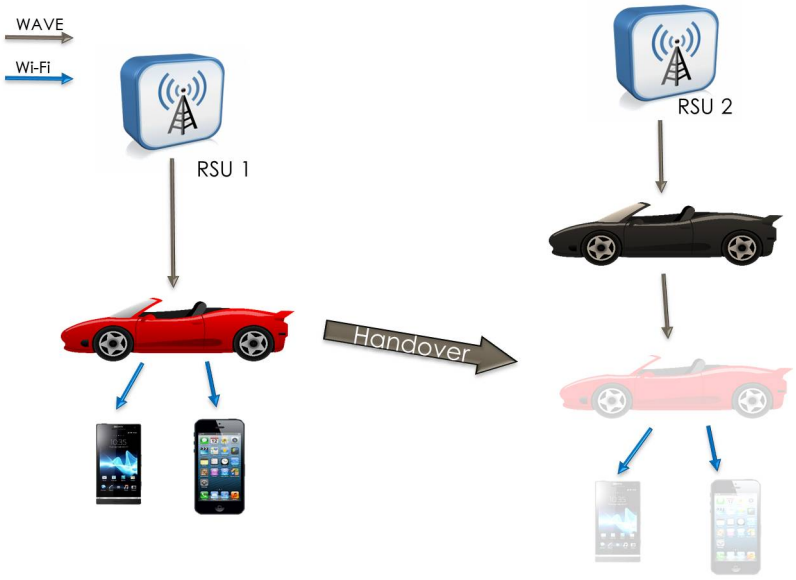


Figure 3.4: Horizontal handover between RSU at different number of hops

As have been seen previously, in order to be able to analyze handover in all these scenarios, it is necessary to equip the mMAGs of intelligence so that they can be able to make handovers as long as they are moving along the roads within range of an access point that can provide them with better conditions than the one where they are connected. For this purpose, a tight interaction between the mobility protocol and the connection manager needs to be provided. Figure 3.5 is a representation of the principle of interaction of the connection manager and the network mobility protocol. The connection manager monitors the connection quality of the existing networks, selects the network which provides better connection quality, and communicates with the mobility protocol server-side triggering the handover at the MAC layer, sends a Router Solicitation (RS). The mobility protocol (server side), after capturing this RS, it starts the registration process of the node and its handover if it was already connected to another network. After completed this process, it sends a Router Advertisement (RA) informing the node of the prefix assigned. Finally, the mobility protocol (client side), after detecting the capture of a new RA, it will configure some of its parameters, such as the IPv6 address, if it has not yet been assigned.

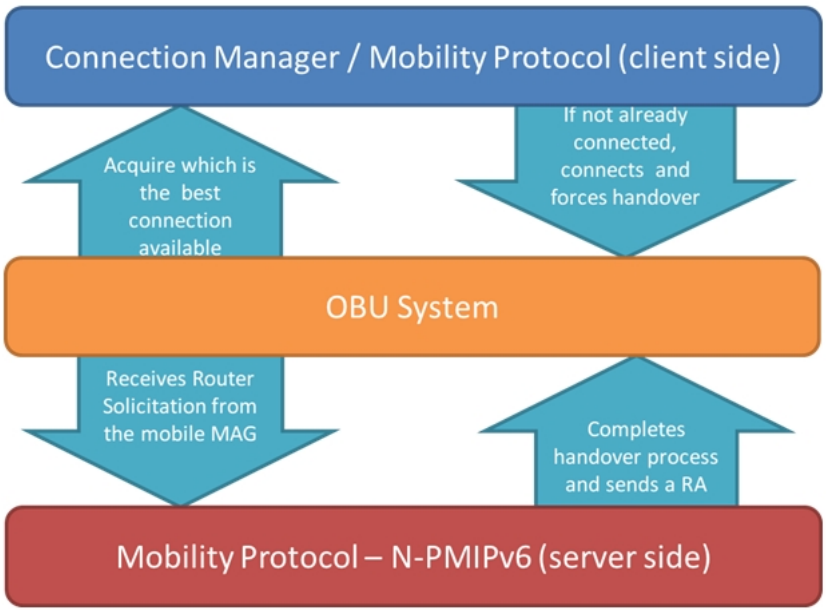


Figure 3.5: Interaction between the N-PMIPv6 and the connection manager

3.3 PMIPv6 Implementation used as a starting point

Since the N-PMIPv6 protocol is a variant of PMIPv6, this was the obvious choice to use as a base and to apply the necessary changes. In order to better understand the changes, first it is important to understand how PMIPv6 works and analyze each of the entities that compose it. The used implementation of PMIPv6 was the Open Air Interface Proxy Mobile IPv6 (PMIPv6 OAI) [19], version 0.4.1, an open source implementation based on the implementation USAGI-patched Mobile IPv6 for Linux (UMIP) [18], version 0.4, the MIPv6 protocol.

The base version used has already been subject to changes in a previous work [11] which consisted on handover process improvements to make it faster and with low connection loss.

A more detailed explanation of the operation method of the PMIPv6 protocol will now be presented.

3.3.1 Operation method

Before explaining the changes made to the PMIPv6 protocol in order to implement the N-PMIPv6 to support network mobility, it is important to understand the way it operates in order to understand what are its limitations, and how it can be extended to provide mobility to a whole network. Thus, in this section it will be explained the operation method

of PMIPv6, as well as the identification and characterization of entities that it comprises. Since the mobility process is started on MAGs, these identities will be characterized first; and the LMA operation will be explained next.

MAG operation method

For a mobility protocol to be effective, it is absolutely required that the motion detection of the incoming nodes be as fast as possible, in order to obtain a reduced loss of connection during the handover. In PMIPv6, the entity responsible for this detection is the MAG and its operation flow diagram can be seen on figure 3.6, which will now be explained.

The OAI PMIPv6 provides two forms of motion detection, one of them is through the association and disassociation generated by Cisco Aironet 1100 series access points (implementation required for a testbed in which these APs were used), and the other is through the RS messages. Thus, the MAG, after completing the appropriate settings configurations, starts the needed captures to catch the referred messages and then enters on a finite state machine that manages the operation of the entity. The MAG is now waiting for an event.

When the motion of a node is detected, the state machine initiates the processing of the received message: it first gets the MN-ID (mobile node identification) through which it checks whether or not there is already a BCE created for this. According to this processing, the following paths can be taken:

- If the MN does not have a BCE, it is triggered the registration process for the new node.
- If the MN has a temporary BCE, then the registration process is finished, creating the tunnel to the LMA and the routes to the MN.
- If the MN already has a definitive BCE, then this is only refreshed.

Now, it will be analyzed the process of registering a new node. If the MN detected does not have a BCE, it means that the MN was not connected to that MAG, and hence it is necessary to register it.

In the implementation of OAI PMIPv6, the nodes validation is performed via a Radius server that will have to be running in a machine accessible by the MAG, usually it is placed

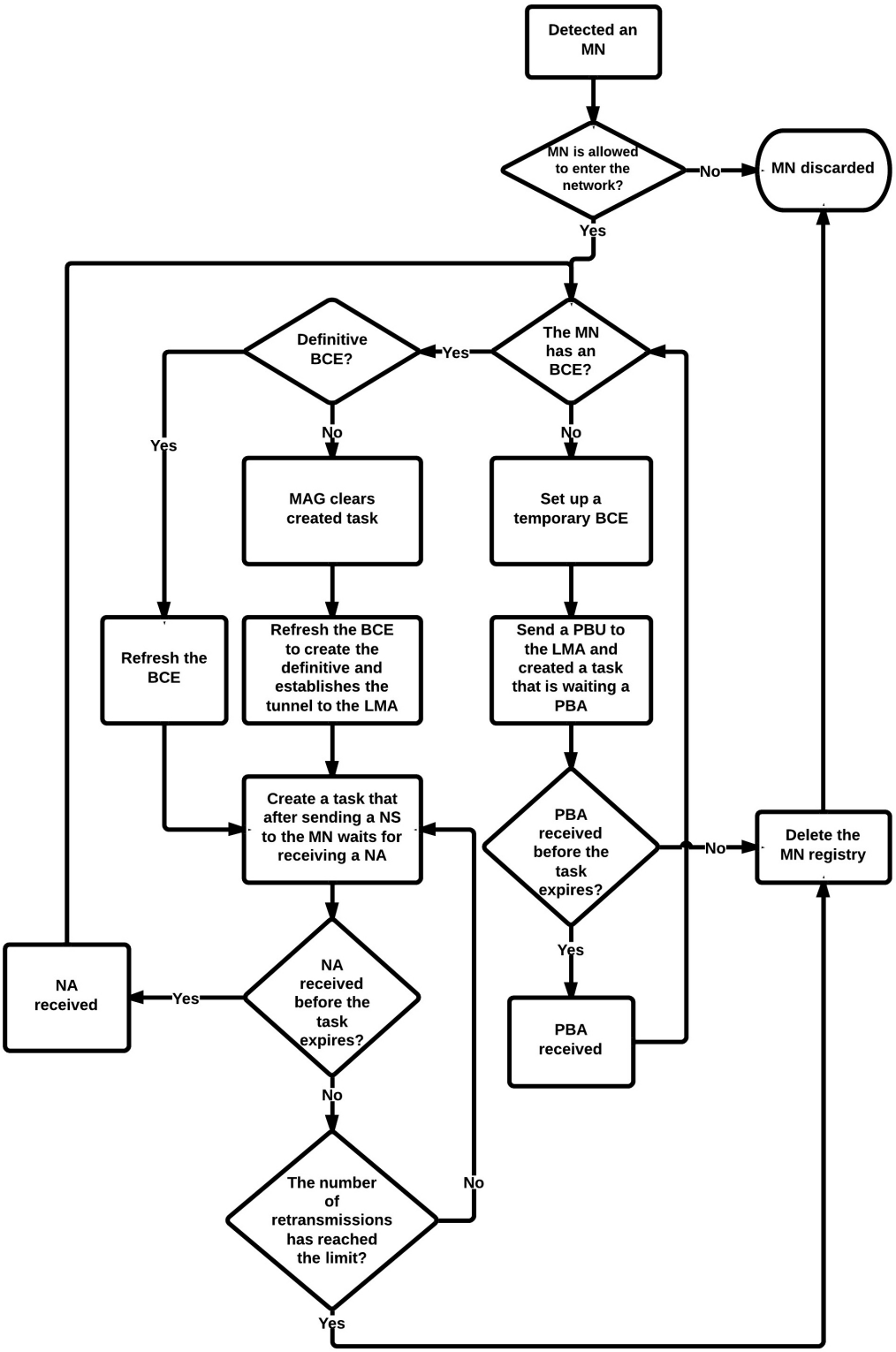


Figure 3.6: MAG operation flow diagram

on the same machine that the LMA. The implementation of the radius server used was the freeradius-client-1.1.6 [41]. When a new node enters the network, it is verified through its MN-ID whether or not it is authorized to connect to the network through a request to the radius server. If the answer is negative, the registration is canceled and the node will not be connected to the network. If the answer is positive, then the function *mag_pmip_md* is called, and it fills all fields of the BCE in accordance with what is defined in the protocol. Then, it is called the function *mag_start_registration* in which it is sent the PBU message to the LMA with information of the new node; the MAG is now waiting the response of the LMA, inserting the BCE of the MN as temporary. If within a pre-defined time-out it is not received a PBA in response to the PBU sent, the BCE is cleared and the registration of the MN is cancelled.

When the PBA is received, the MAG goes back to the finite state machine, but as this time the BCE is temporary, and it is called the function *mag_end_registration* that makes the BCE definitive and creates a task that periodically sends Neighbor Solicitation messages to the MN to confirm if it is still within reach or not, depending on whether it receives answers to these requests (through Neighbor Advertisement messages) or not. To complete the process, the tunnel between the MAG and the LMA is created for directing traffic to and from the MN, and at last it sends a RA message to the MN, through the function *mag_kickoff_ra*, indicating the home network prefix (HNP) that has been assigned to it. At this point, the registration of the MN is completed.

As mentioned, after the registration is complete, the MAG will keep the BCE of the MN, while it is at his range checking it by sending periodic NS messages. For this purpose, it starts the *ndisc_send_ns* function and then waits for an NA message sent by the MN as response. After a pre-defined time out, if the response is not received, the MAG resends the request. If after a pre-defined number of attempts the MAG continues to get no response to NS messages, it assumes that the MN is no longer at his range and initiates it's deregistration. This consists in eliminating the MN's BCE, reduce the number of users of the communication tunnel to the LMA (if the number of users reachs zero, then the tunnel is removed), removes the route to the MN, and finally a PBU message is sent to the LMA indicating that the MN has left the MAG. On the other hand, if the MAG receives the response to the sent NS message, then it re-enters the state machine and this time, as the BCE is definitive, it is only made its update being invoked the *mag_end_registration_no_new_tunnel* function which procedure is very similar to the *mag_end_registration* function that was invoked when the MN was still being registered, differing only in that it is no longer necessary to create the tunnel and routes for the MN because they have already been created.

LMA operation method

According to the PMIPv6 protocol, the LMA is the entity responsible for managing mobility, and it must keep a record of the current location of each MN connected to the network. Its operation flow diagram is depicted in figure 3.7 and will now be explained.

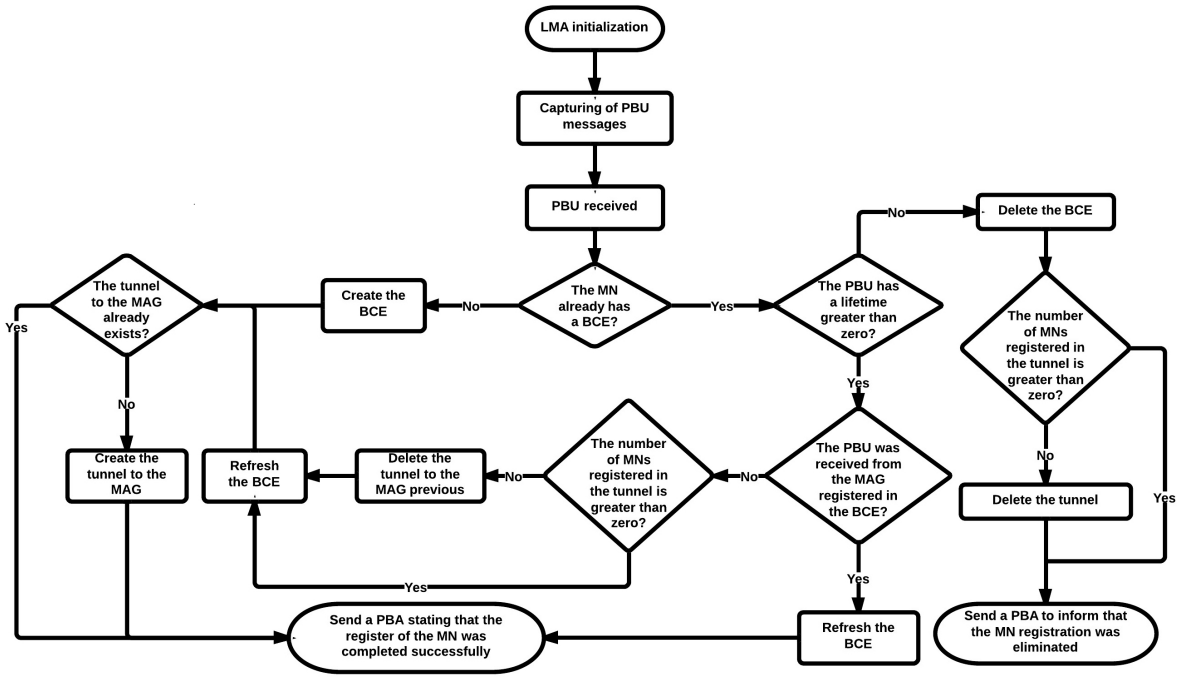


Figure 3.7: LMA operation flow diagram

The LMA operation is also based on a finite state machine. As all the motion detection is performed by the MAG, the LMA only has to receive and process the PBU messages sent by them; therefore, after booting and running the necessary configurations, the LMA starts capturing PBU messages.

When a PBU message is captured, the program proceeds to the state machine from where it can go for one of two paths:

- Registration of a new MN, if the MN that triggered registration does not have yet a BCE.
- Update of the MN BCE, if the MN that triggered the registration already has a BCE.

In the case the MN does not have a BCE, the registration of the new MN starts following a similar procedure than in the MAG: it is created and filled in the BCE according to the

specifications of PMIPv6 and information constituting the PBU, it is created the tunnel between the LMA and the MAG, and then routes are established to the MN. To complete the registration, a PBA message is sent to the MAG in order to complete the registration of MN.

If the LMA receives a PBU corresponding to a MN that has already a BCE, then the first step is to check whether the MAG sending the PBU is the same as the one identified on the BCE, in which case it would merely be updated. If it is not, then it is a situation of handover between MAGs. In this situation, the LMA eliminates the previous BCE of the MN and the old tunnel and routes referring to the old MAG, and then normally registers the MN as if it were a new MN.

3.3.2 Modifications in previous work

In a previous work [11], the OAI PMIPv6 version described above has already been subject to some modifications in order to support the handover procedures more efficiently. The changes made were:

- Adaptation of the protocol in order to support *sit* interfaces (IPv6-in-IPv4) to enable the utilization of the cellular networks as the access technology.
- Change the way MAG registers the mobile node in order to accelerate the process which will allow reducing the time of handover.
- Change the way LMA processes MN handover between different MAGs.

With a fully operational PMIPv6 protocol, it is now possible to start implementing the N-PMIPv6 protocol. However, we detected several issues on the integration with the WAVE/DSRC technology, and on the support of WI-FI sharing and broadcasting with the same physical interface. The next section will explain and describe the implemented solutions to these problems.

3.4 Interaction between the Wireless technology and the Mobility Protocol

With the progress of the experimental tests of the PMIPv6 mobility protocol, some adverse situations resulting from incompatibilities between the protocol and the wireless technologies have emerged. This is a result of the unique features that the wireless technologies have in relation to one another. The problems encountered were the following:

- The procedure of sending/receiving the Router Solicitation/Advertising messages does not work as expected in the IEEE 802.11p technology. This is due to the fact that this type of messages has been developed over a set of assumptions that are true for IEEE 802.11g but are not for the IEEE 802.11p.

- The way the mobility protocol expects the Neighbor Solicitation / Advertisement messages to be processed does not work properly with the IEEE 802.11p technology. This is also due to the fact that this type of messages has been developed over a set of assumptions that are true for IEEE 802.11g but are not for the IEEE 802.11p which affects its behavior.

- The IEEE 802.11g physical interface is not supposed to be used to receive and broadcast a WI-FI network at the same time. Since we need this double role to be able to access to a WI-FI hotspot and simultaneously disseminate a WI-FI network in the car, a virtualization approach is envisaged.

A more detailed description of the problems and the solution adopted will be now presented.

3.4.1 The IEEE 802.11p and the Router Solicitation/Advertisement messages

Both the MAG of the PMIPv6 protocol as the mMAG of the N-PMIPv6 give start to the register of a new node, which connects to its network, when it receives a RS message from the mobile node indicating its intention to connect to the MAG/mMAG. After the registration on the MAG/mMAG and on the LMA is completed, it is then sent a RA to the mobile node with the prefix which has been assigned to it.

The RS is an ICMP message sent to a specific multicast address, the ff02::2 [4]. Therefore, the MAG/mMAG should answer to any RS received whose target address is this one. Technologies with session establishment, such as the IEEE 802.11g, work well with this approach, because if the mobile node is connected to MAG/mMAG by this technology, then it is guaranteed that the packets sent by the mobile node will only be received by the MAG/mMAG with which it is associated, even if there are other MAGs within range.

With IEEE 802.11p technology a problem arises, since there is no prior session establishment on association by the user (mobile node) to the provider (MAG/mMAG). When the user sends the RS message to the multicast address ff02::2, all the MAGs will receive this message and how it is pre-defined; on receiving an RS which destination address is

ff02::2, they will start the registration assuming that the node does indeed require connection to them, when in fact it should only be received by the MAG to which the provider is associated to the user of the mobile node, figure 3.8. This makes the LMA receive location updates of the mobile node from multiple MAGs which will end up on repeatedly move the *ipv6_tunnel* used to forward the messages between the multiple MAGs. The problem is that the mobile node has registered as a user of the provider of a specific MAG; therefore, only on a short time interval, in which the LMA has correctly assumed that the route is established through that MAG, it will be possible to correctly forward the messages.

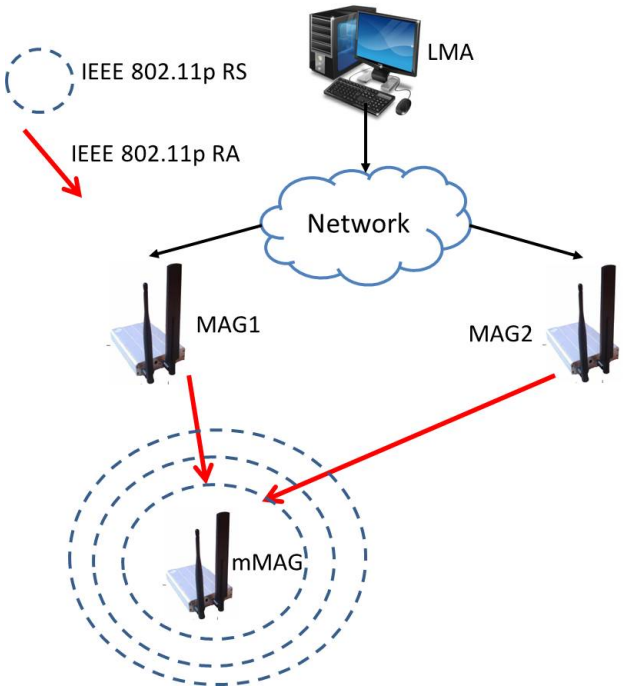


Figure 3.8: Router Solicitation problem

In order to solve this problem, the way how the Router Solicitation/Advertising messages are processed and sent was modified. For this, purpose a careful study of the source-code of the program used by the connection manager for sending the RS was carried out.

The user space program is called *rdisc6* and enables sending RS messages through a particular interface, using the command: "*rdisc6 <interface name >*" and is part of a package called *ndisc6* that, besides this feature also enables sending Neighbor Solicitation (NS) messages for a given link local through a given interface, i.e., using the command: "*ndisc6 <link local> <interface name>*" [1].

After analyzing the source code, we concluded that, in order to support both types of

command entries required for sending the NS and RS, the RS should always be sent to a multicast address pre-defined, while the NS should be sent to the link local specified in the command line. It turns out that, even if the command is a *rdisc6* (not the *ndisc6*), if more than one argument is specified (not just the destination interface) then it wrongly assumes that the first is the destination link local (replacing the pre-defined multicast address) and the second argument will then be assumed as the destination interface.

In short, if the connection manager wants to send a RS using the rdisc6 program, then it needs to use the following command: *rdisc6 <link local> <interface name>*

Thus, if one mMAG wants to connect to another MAG/mMAG through the IEEE 802.11p technology, it has to send an RS explicitly directed to the desired provider, which will now be the only to answer, this eliminating the problem mentioned above, as can be observed in figure 3.9.

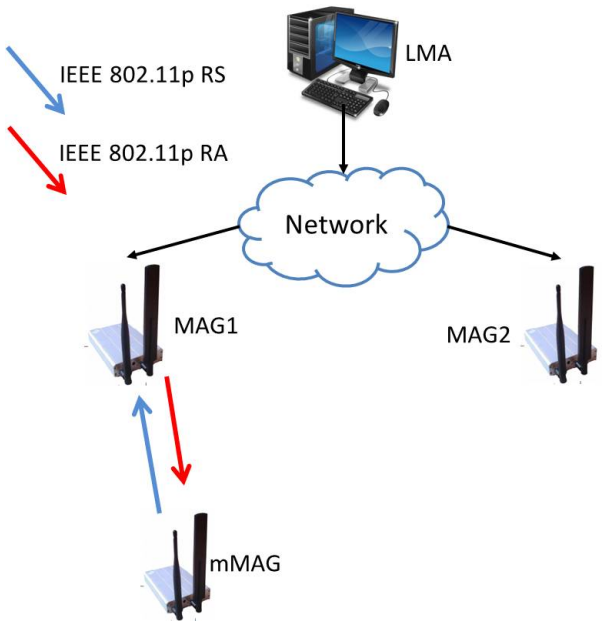


Figure 3.9: Router Solicitation problem solution

3.4.2 The IEEE 802.11p and the Neighbor Solicitation / Advertisement messages

As explained in the previous section, as there is no session establishment in IEEE 802.11p, the messages sent are received by all the MAGs at range. For example, if the mMAG is now the user of a provider of a specific MAG, if there are other MAGs on range,

when the NS messages are sent they will receive them and respond accordingly.

The problem arises from the fact that both of the mobility protocols, the N-PMIPv6 and the PMIPv6, are based on the periodic transmission of NS messages to the mobile nodes connected to be able to verify if they are still connected to each other or not. When a mobile node, for example a mMAG, moves from a MAG1 to a MAG2, it starts its registration in MAG2 by sending a RS and everything proceeds accordingly. However, when MAG1 tries to send an NS for the mMAG to see if it is still linked to it or not, the mMAG, even though now it is the user of the MAG2 and not of the MAG1, it will receive the NS and will respond to it with a NA, and the MAG1 after receiving this NA assumes that the node is still attached to it, and therefore sends a PBU to the LMA in order to make a refresh of the BCE. When the LMA receives the PBU from the MAG1, it assumes that the mMAG is again attached to the MAG1 and then changes the route to forward the traffic through the MAG1. Yet, the mMAG is still a user of the provider announced by the MAG2, so it will not be possible to forward the traffic to it through the MAG1 and the connection is lost, as can be observed in figure 3.10.

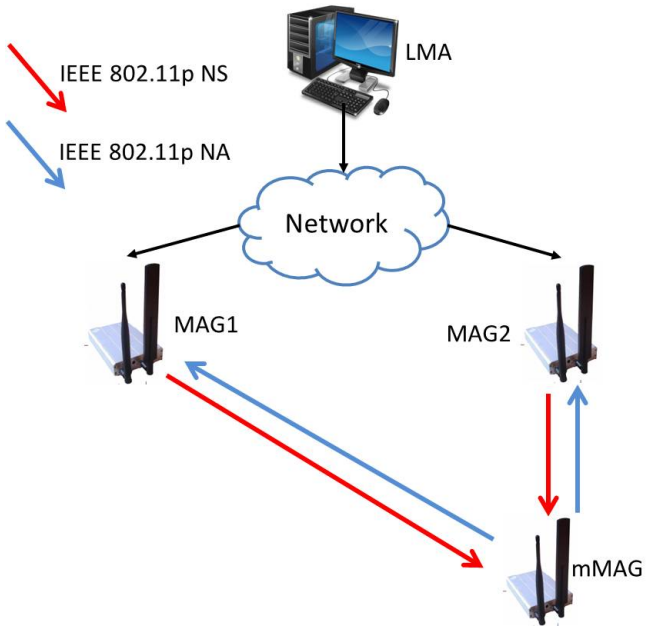


Figure 3.10: Neighbor Solicitation problem

This problem can be solved if the mMAG, when moving from the MAG1 to the MAG2, starts to reject all the NS messages which source is the MAG1. That way, the MAG1 will not get any response to the sent NS messages, then assuming that the mMAG is no

longer connected to it, processing its deregistration. The adopted solution is conceived through the functionalities of the *IP6_TABLES* module that allows to drop packets of a given ICMPv6 type from a given link local. Each time a mobile node moves from one MAG1/mMAG1 for another MAG2/mMAG2, it should record in the ip6tables an order to accept NS packets from the MAG2/mMAG2 and reject those from MAG1/mMAG1, as can be shown in figure 3.11.

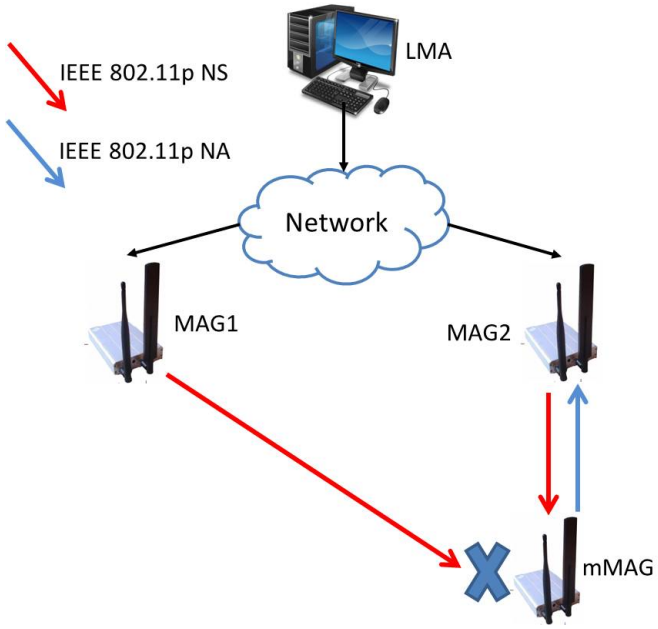


Figure 3.11: Neighbor Solicitation problem solution

3.4.3 The IEEE 802.11g and the sharing of the physical interface

One of the objectives of this Dissertation is to enable users within the vehicles to access the Internet as they normally do in their daily life, i.e., connect to the Internet using one of his personal devices, cellphone, tablet, laptop, or any other device with WI-FI capabilities, by simply connecting through the access point provided by the OBU. On the other hand, the OBU needs to be able to perform handover between networks of different technologies, one of them is the IEEE 802.11g (WI-FI). In this case, there will be times when the OBU must be able to be connected to a WI-FI network through which it connects to the Internet, and at the same time it will have to broadcast and maintain a WI-FI network to its users inside the car. Ideally, the OBU should have a single IEEE 802.11g interface that needs to be shared by both processes described before.

The same functionality is required in the IEEE 802.11p interface, which is also expected to be able to be a user and a network provider at the same time; however, this technology is able to perform this role, and therefore, having only one interface does not create any problem.

Returning to the IEEE 802.11g interface, it was found that this was indeed impossible, because the fact of having the interface broadcasting a network makes it impossible to use that same interface for connection to other networks while on the move. The only way to deal with the problem is to create a virtual interface over the same physical interface; one of them is used to broadcast a network to the users within the vehicles, and the other is used to search and connect to the available access points in order to maintain the access to the Internet.

This has some improvements comparing to the initial situation, as it is now possible to search and connect to the other interfaces without the need of turning off the network which is being broadcasted within the vehicle. However, it is only possible if it is switching to an access point transmitting in the same frequency channel that is being used on the broadcast network. For example, if it is being broadcasted a network on the channel 4, if it wants to connect to an exterior access point transmitting on the same channel, there is not a problem, but if it wants to connect to an access point transmitting on channel 6, it will have to shut down the broadcasted network, then connect to the access point and finally restart the broadcasted network, but now using the same channel from which it is receiving from the exterior access point.

Another problem is that, during the operation of scanning to find out if there are any available access points, the physical interface is blocked, and therefore even if there are users receiving Internet (the mMAG is receiving it from a WAVE connection), as they are connected to the OBU by the WI-FI interface they will not be able to receive any traffic, they look connected but they actually are not. This limitation of the IEEE 802.11g technology brings some problems that cannot be solved without recurring to an extra IEEE 802.11g interface. However, the virtual interfaces method was the adopted solution because it partially solves the problem and this way, the OBU does not need any extra interfaces.

3.5 Implementation of the N-PMIPv6 mobility protocol

In the PMIPv6 protocol the MAGs are static entities, whose addresses are pre-defined; moreover, they must have a direct connection to the LMA not allowing chaining MAGs. On the other side, as the MAGs manage their subnets, if they do not have mobility,

consequently their private networks cannot be mobile.

Since the purpose of this Dissertation is to provide mobility to the OBUs and to the users connected to the OBUs, the PMIPv6 must be modified in order to support network mobility. Moreover, it is also our purpose to extend the range of the RSUs/APs connection allowing mMAGs to connect to other mMAGs in order to form a chain, and thus increase the range of the Internet access. For this purpose, it is necessary that the mMAG be capable to configure itself according to the access point via which it is connected. Thus, the PMIPv6 MAG must be modified to acquire these characteristics.

The necessary changes will now be identified and will be better described in the following sub-sections:

- LMA must be able to recognize mMAGs and be able to create tunnels to these as if they were normal MAGs.

- The MAG must be able to identify whether it will intercede as a static or as a mMAG.

- If it has to operate as mMAG, the MAG has to be able to identify its IPv6 prefix assigned on the network to which it is connected, in order to configure its own IPv6 address, so that it will be able to communicate with the LMA and therefore the Internet.

- As a mMAG, it must also have a RS filtering system, or otherwise it would, for example, receive and process its own RS, since the mMAG, being mobile, requires sending these packets to the network to which it is connected. This was explained in sub-section 3.4.

3.5.1 LMA tunnel creation to mMAGs

The changes to be made in the LMA are simple, since its operation relatively to a MAG/mMAG remains the same. However, it is found that the chaining of MAGs will cause problems in establishing the tunnel for these due to a verification performed.

In this verification, if it is detected another existing tunnel for a mMAG earlier in the chain than the current one, and the request to create the tunnel is discarded, as can be shown in figure 3.12. To solve this problem, this verification was eliminated, which does not affect the correct operation of the protocol.

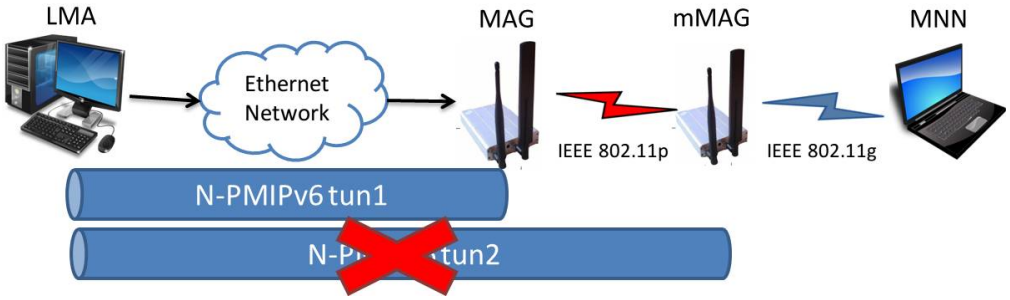


Figure 3.12: LMA multi tunnel problem

3.5.2 MAG and mMAG Identification

The MAG needs to be able to identify whether it has to behave like a static or a mMAG. In case of being a mMAG, it will have no previously fixed address assigned, so it must be able to receive and process RA messages (resulting from the RS messages sent by the connection manager).

For this propose, it is necessary to first define a configuration method that allows the MAG to distinguish if it will act as mMAG or not. As discussed previously, a feature of the fixed PMIPv6 MAG is that it has a pre-configured IPv6 address. To implement the protocol N-PMIPv6, it is assumed that, if in the configuration file it is assigned a static address to the MAG, then it will behave as a fixed MAG; if no address has been pre-configured then the MAG behaves as a mMAG.

In order to be able to perform this process, it was first necessary to determine which IPv6 address is assigned by default when it is not present in the configuration files. It was found that the IPv6 address assigned by default is the loopback address 0::1/128 [4]. To make easier to access to the information, if it is or not a mMAG, it was created a flag on the MAG configuration struct(*mip6_ config* struct) named isMR ('is a Mobile Router'). This flag will be set if the IPv6 address of the communication interface with the LMA (MagAddressEgress) is equal to the loopback address, because this indicates that this was not defined into the configuration file, and therefore, it is a mMAG. This assignment is not made if the entity is an LMA.

From this point on, it is possible throughout the remaining process to distinguish when the node shall act as a static or mMAG based on the value of the flag isMR.

3.5.3 MAG configuration from a received Router Advertisement

If the MAG will act as a mMAG, it has to have the ability to receive and process the RA directed to it and, based on their information, configure its own IPv6 address in order to be able to communicate with the LMA. The necessary changes are the following:

- Create and register a handler that will be initialized whenever a RA packet is received in order to make its processing and act accordingly.

- To accomplish this, a function named *pmip_mag_recv_ra* was created. It takes as arguments the ICMP bit stream and the source and destination addresses. After parsing the message, it will upgrade or not the IPv6 address of the interface depending on which is the return value of the parsing function.

- To register the handler, it was used the function *icmp6_handler_reg* in which the argument is the message type that is aimed to be captured (in this case it is *ND_ROUTER_ADVER* and also the name of the handling function (the *pmip_mag_ra_handler*, which makes the link to the handling function implemented, the *pmip_mag_recv_ra*). As this is only needed if the entity is a MAG, the registration is made within the *pmip_mag_init* function which is only called if it is a MAG/mMAG, and since even among MAGs this feature is only useful if it is a Mobile MAG, an additional check is included which ensures that the registry is only done if the isMR flag is active.

- Create a function to do the parsing of the RA byte stream translating its multiple fields in order to make their access easier. For this purpose, it is created a function called *icmp_ra_parse* (on the module *pmip_msg.c*) which receives as arguments the ICMP byte stream captured, the source and destination addresses and the structure which will be filled with the information received in the RA (one of the most important is the prefix that has been assigned to the mMAG).

3.5.4 Mobile MAG implementation

With the modifications detailed in sections 3.5.1 to 3.5.3, it is now possible to implement the mMAG of the N-PMIPv6 protocol. Since its operation method will be very similar to the one of the MAG of the PMIPv6 protocol, the PMIPv6 MAG will be used as basis. Indeed, the mMAG is an entity that comprises the functions of both fixed MAG and mMAG. Its operation flow diagram is depicted in figure 3.13 and will now be detailed.

When the mMAG is initialized, it starts evaluating if it will work as a fixed MAG or

as a mMAG; this procedure makes sure that only the necessary modules and captures are initialized.

If the MAG is supposed to work as a fixed MAG, then only the PBA and RS captures are initiated. When a message is captured, it is evaluated from which interface it comes from. If it is captured by the WAVE interface, it will then be verified who its destination is. The message will be accepted only if the destination is this particular fixed MAG. It will prevent the fixed MAG to answer to RS messages sent to the broadcast address, which result in the problem of WAVE technology and RS messages, as was detailed section 3.4.1. If the message is accepted, it is now started the regular MAG of the PMIPv6 protocol. Therefore, all the necessary functions have been migrated from the PMIPv6 implementation used as a starting point.

If the MAG is supposed to work as a mMAG, then not only the PBA and RS are initiated, but also the RA captures are initiated. Since the mMAG has no interface address yet assigned, it will have to configure it from the incoming RA messages. Those messages will be triggered by a connection manager responsible for selecting the attachment point of the entity (this will be detailed in section 3.7). If a RA is captured, the mMAG calculates the address assigned by joining the prefix received on the RA message with its own link local address. To accomplish this, the modifications detailed in section 3.5.3 are performed. After the first time it receives and processes an RA, the mMAG is a fully function MAG, as if this is a regular fixed MAG. When the mMAG receives a RS, it follows the same procedure than the fixed MAG: first it checks from which interface it comes, and if the message is valid, it proceeds to the mobile node registration which procedure is the same as in the PMIPv6 protocol (and has been described in section 3.3).

The next sub-section will detail the handover process implementation.

3.5.5 Handover process

Due to the abstraction on the way this code has been developed, everything else works the same way for both MAGs and Mobile MAGs since, as happens in PMIPv6, a route connecting the MAG/mobileMAG to the LMA is guaranteed. In other words, if it is ensured that the mMAGs always obtain valid routes throughout its displacement between different access points (other MAGs), then their behavior will process normally and the mobility of the users is ensured. It is thus possible, with very subtle changes to the PMIPv6, to separate the MAG between its mobile and static role.

In fact, the way in which the N-PMIPv6 will operate is similar to a cluster PMIPv6 network: a mMAG1 is a common user for the MAG which is providing connection, and

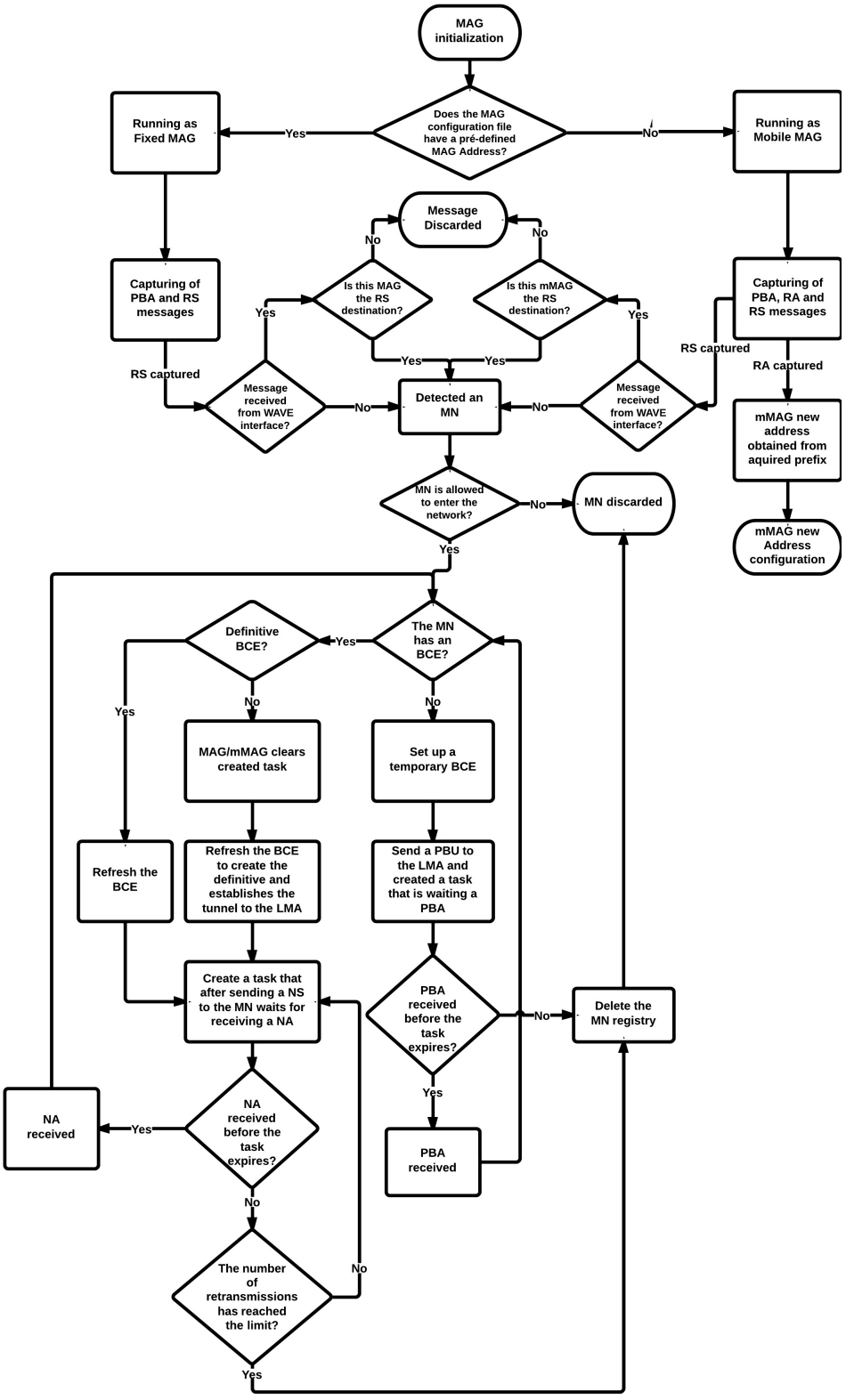


Figure 3.13: Mobile MAG operation flow diagram

another mMAG2 which wants to connect will also be treated as a simple client for the mMAG1. The maintenance of the link/route for the LMA is guaranteed jointly with the connection manager, which forces the connection to the network that offers the best conditions.

The figure 3.14 is an example to better understand the process.

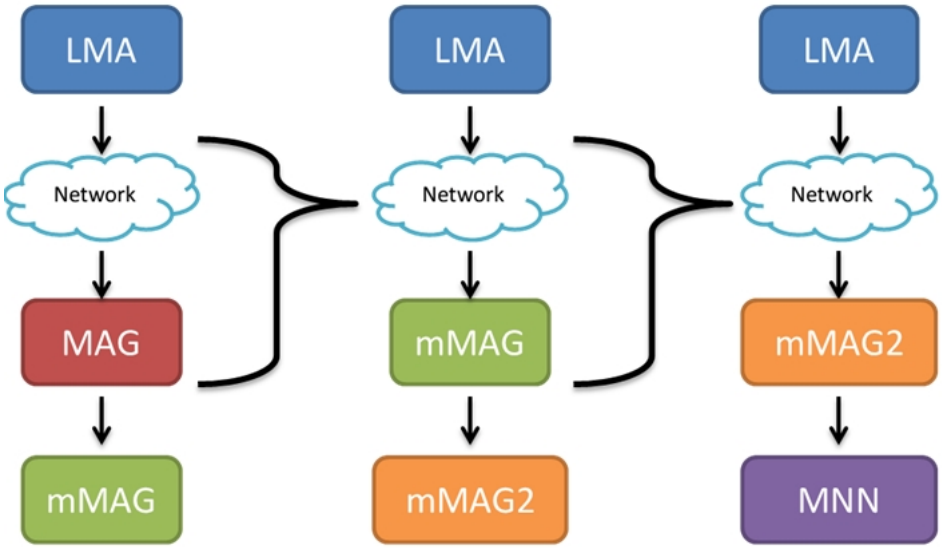


Figure 3.14: N-PMIPv6 network abstraction

The example on the left side of the figure 3.14 is the basic principle of PMIPv6: the mMAG is seen as a regular user to the MAG to which it connects and it is registered normally. From this moment on, it is guaranteed, regardless of the PMIPv6 MAG that binds this node, that this has ensured mobility and an active route to the LMA. As has been referred before, this is the pre-requisite for a node to be able to act as mMAG. Then, it is assumed that the mMAG is indeed a fully operational MAG, and all that stands between the mMAG and the LMA is only network routing, and packet forwarding. Therefore, as can be seen in the center part of figure 3.14, another user (in this case another mMAG, mMAG2) will bind to mMAG as if it was a standard PMIPv6 registration, so the mMAG2 will then also get an IPv6 address, and it has guaranteed mobility between MAGs, and a route to the LMA. Again, we can conclude that this mMAG2 is now a fully functional MAG, and it may also serve other users, as it is shown in the right part of the figure where it registers another mobile node. In this way, N-PMIPv6 can support mMAGs chaining, which can significantly increase the coverage of the RSUs using multi-hop across the chained mMAGs, providing Internet access to users over a greater distance.

However, network mobility must also be ensured. Let's consider the example of the figure 3.15, to remember how the mobility of a user in PMIPv6 protocol is processed.

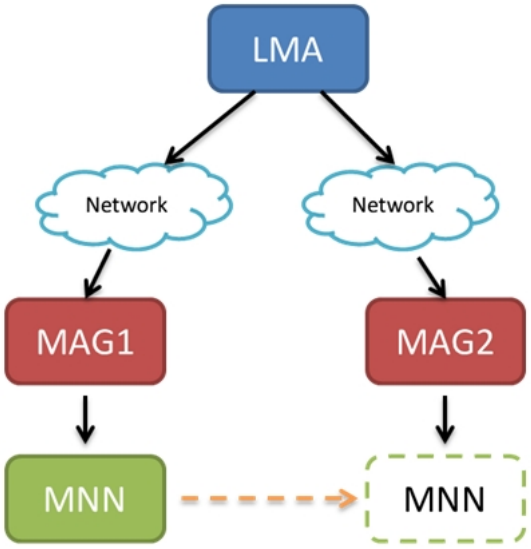


Figure 3.15: PMIPv6 handover representation

The MNN is registered in MAG1 and the LMA has now a route in which it is stated that, to route packets to the MNN, they should be sent through the MAG1. When the MNN performs handover from MAG1 to MAG2, the information in the LMA is updated and now it knows that it has to send packets destined to MNN through the MAG2. Keeping this principle and since, as we have seen in the previous point, the mMAG is treated as a normal user by the MAGs to which it is attached, it is ensured the mMAG mobility, as confirmed in figure 3.16.

At this point, the LMA has a valid route to the mMAG regardless of whether it is connected to MAG1 or to the MAG2. Now, let's consider an example in which the mMAG has a dependent network as can be observed in figure 3.17.

Before the mMAG handover, the LMA has a route to the mMAG through the MAG1, resulting from the registration of the mMAG on the MAG, and it also has a route for the MNN1 and MNN2 through mMAG which results from the registration of these mobile nodes on the mMAG. Therefore to forward packets to the mobile nodes, the LMA can conclude that it should send them through the mMAG, because the mobile nodes are its dependents, since the LMA knows that it has to send them through the MAG1, then the route to follow is represented on figure 3.18.

After the handover of the mMAG from the MAG1 to the MAG2, the LMA will now

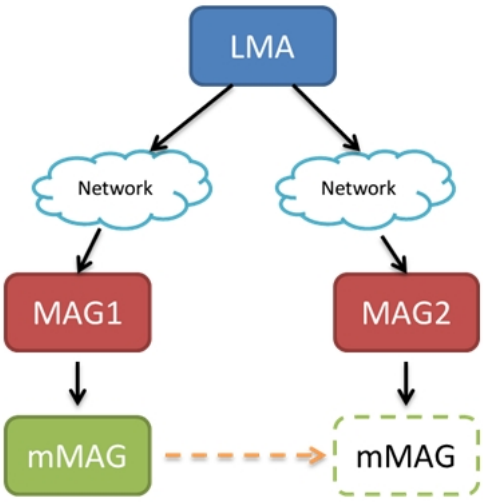


Figure 3.16: N-PMIPv6 mMAG handover representation

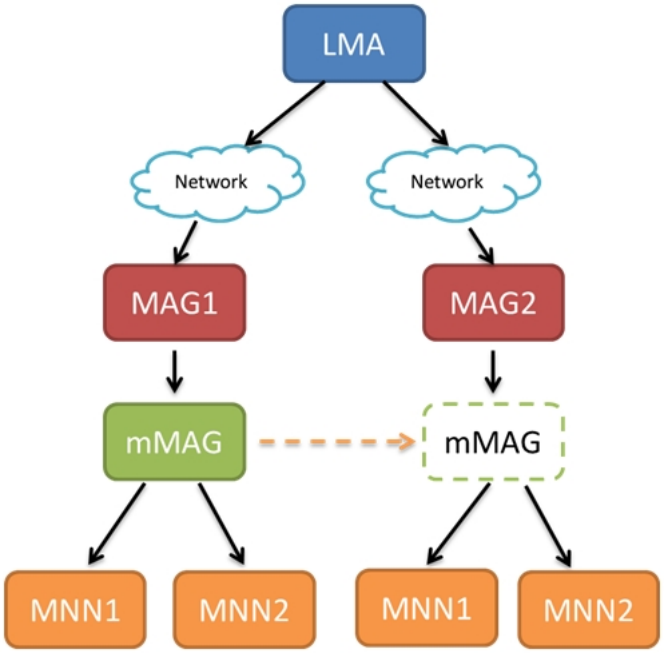


Figure 3.17: N-PMIPv6 (mMAG and dependent network) handover representation

---

know that to get to mMAG, it must now forward the packets through the MAG2. Similarly to the above, the LMA can conclude that for forwarding packets to the mobile nodes which are connected to the mMAG which are now connected to the MAG2, the route to take is represented on figure 3.19.

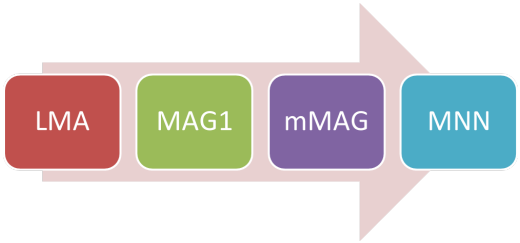


Figure 3.18: Path to MNN before handover

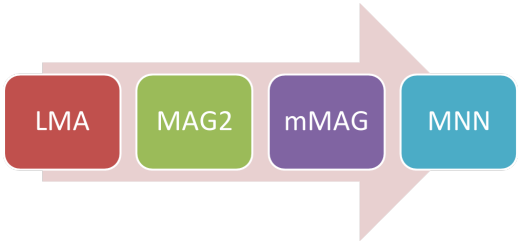


Figure 3.19: Path to MNN after handover

This process works regardless of the number of mMAGs chained, because it is a recursive process. With this process, it is then guaranteed the network mobility supported by N-PMIPv6. Note that all this is done in the most efficiently way: to shift an entire network, it is only necessary to move its point of connection, the mMAG, so it is not needed to update the entry of all the users: all that is required is to update the entry of the mMAG. The total cost in terms of number of handovers is the same as in PMIPv6.

All these procedures are performed as described on the N-PMIPv6 draft [24].

3.6 IPv4 over IPv6 Internet

In order to be able to connect a normal user in a real environment, it is expected that the vehicular networks, in addition to the applications made especially for them, also have the ability to share normal Internet access. Thus, the user within the car can connect to the available access point and access his email, social networks, games, just like he does at home or workplace. The problem in this support is that the majority of the existing personal devices only support IPv4 networking. Since the mobility protocol developed only supports IPv6 mobility, it would be impossible for the user to enjoy this service. To compensate for this issue, it is implemented a system that provides mobility to the users with IPv4 terminals.

The mobility protocol developed ensures that, even if the OBU / mMAG moves between different access points, it keeps connected with the rest of the N-PMIPv6 network. Under this assumption, it is guaranteed that the OBU while travelling along will keep a stable connection to the midpoint of the network, the LMA. Assuming that the LMA has IPv4 Internet connection, which is very likely, it is possible to create a system that allows the MNNs to use this link. This system is composed by a IPv4-in-IPv6 tunneling system between the mMAG and the LMA, to where it is redirected the traffic from the IPv4 network broadcasted by the mMAG that targets addresses not belonging to that network, and a NAPT server (Network Address and Port Translation server) to run in parallel with the LMA, on the same machine, which will convert all requests originated on the mMAG network as if they were made by the LMA itself [48]. When the response to these requests is received, the NAPT server back resets the original address and sends it over the established tunnel. In the figure 3.20, it is represented the process.

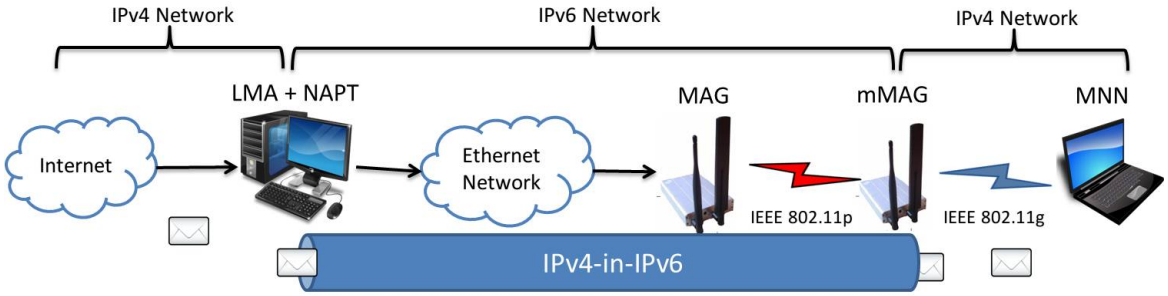


Figure 3.20: IPv4 Internet enabling system

Since the mobility of the mMAG is guaranteed by the developed mobility protocol, it is then also ensured the mobility of the IPv4 users while they are enjoying the WI-FI network available. It is not possible, however, to ensure the mobility of users if they move between different mMAGs, and as such, it is not possible to ensure full mobility to users in IPv4. However, this is already a significant improvement to apply network mobility for IPv4 users in VANETs.

3.7 Connection Manager Implementation

In order to automate the process of handover of the vehicles along their journey, it is necessary that they have a system capable of monitoring the available networks at their range and trigger the handover to the network that provides the best conditions. Before

explaining the connection manager implementation, it is important to first analyze what is necessary to perform the handover and what are the metrics that identify what is the best available network.

To perform the handover between MAGs/mMAGs, it is necessary (as has been seen in section 2.8.5), that the new MAG receives an RA from the node that is in motion, which will trigger the N-PMIPv6 protocol to proceed with the handover. The connection manager shall then be able to choose the best among the available networks, regardless of access technology, and in case the choice is not the network that is already connected, it shall proceed with sending a RA message to the selected network and changing routes to forward the traffic accordingly. The command format for sending the RA will differ depending on the access technology because, as has been seen in section 3.4.1, the send RA function has a different behavior when to send to a network which access technology is the IEEE 802.11p.

To determinate which is the best available network, it is necessary to make some considerations. The work developed in this Dissertation has taken, as the only measure, the RSSI of the received signal, i.e., the network chosen will be the one which has the highest RSSI. However, this is a very simplistic approach and it is expected that in the future, the network selection should be based on many other metrics, such as speed and direction of the vehicle, bandwidth of the links, expected range of the link, link congestion, etc. Such a connection manager has been defined and evaluated in a parallel Dissertation in the same research group.

Having established these assumptions, it will now be detailed the implementation of the connection manager. It is divided in three modules: the module *gFunctions.c*, which implements the functions to detect and connect to IEEE 802.11g networks; the module *pFunctions.c*, which implements the functions to detect and connect to IEEE 802.11p networks; and the module *connection_ manager.c*, which implements the operation method of the connection manager. These modules will now be detailed.

3.7.1 IEEE 802.11g networks detection and connection module

This module implements the functions of detection, treatment, connection and disconnection with IEEE 802.11g networks. They are the following:

- `gScan`: This function performs a scan to detect which IEEE 802.11g networks are available, returning the identification of the network that has the highest RSSI.

- `gConnect`: This function receives the identification of an IEEE 802.11g and proceed

with the connection to that network.

- `gDisconnect`: This function performs the disconnection of the IEEE 802.11g network that was currently connected.
- `gLink`: This function checks if the node is currently connected to an IEEE 802.11g network.
- `gCheckSignal`: This function returns the value of the RSSI of IEEE 802.11g to which it is currently connected.

3.7.2 IEEE 802.11p networks detection and connection module

This module implements the functions of detection, treatment, connection and disconnection to IEEE 802.11p networks. They are the following:

- `pScan`: This function performs a scan to detect which IEEE 802.11p networks are available, returning the identification of the network that has the highest RSSI.
- `pConnect`: This function receives the identification of an IEEE 802.11p and proceeds with the connection to that network.
- `pDisconnect`: This function takes as argument the index of the IEEE 802.11p network from which it wants to disconnect, and then proceeds with the elimination of that user.
- `pLink`: This function checks if the node is currently connected to an IEEE 802.11p network.
- `getPSID`: This function returns the PSID of the provider that the node is currently connected.

3.7.3 Connection Manager operation module

This module implements the functions related to the operation of the connection manager. They are the following:

- `send\_rs`: This function sends a RS message through the indicated interface for the link local specified in case it is passed as an argument; otherwise, if will be sent to the pre-defined local link.

- `string\_to\_mac`: This function is only for internal handling of data, and it is used to convert a string to the usual format of a MAC Address.

- `mac\_to\_linklocal`: This function returns the link local extracted from the indicated MAC address.

- `iptable\_drop`: This function makes the configuration of the *IP_ TABLES* to force the drop of NS messages from a given local link through a given interface.

- `iptable\_accept`: this function makes the configuration of *IP_ TABLES* to force the accept of the NS messages from a given local link through a given interface.

- `route_add`: this function configures the default route through the interface and link location indicated.

- `route_del`: this function removes the default route through the interface and link location indicated.

- `main`: this is the main function of the module and contains a loop that periodically checks which is the best IEEE 802.11p and connects to this, in case it is not the one that is already connected. Likewise, it connects to the best IEEE 802.11g network and, according to which of them has better RSSI, it routes the traffic for the chosen interface/technology. Comparing the RSSI of both the connected networks, the WAVE and the WI-FI networks, it now selects the one with higher RSSI and starts its configuration. After setting the routes and configure the *IP_ TABLES* in order to only accept messages from the desired interface, it sends a RS message to the network to which it is connected triggering the handover if necessary. All this process is depicted in figure 3.21.

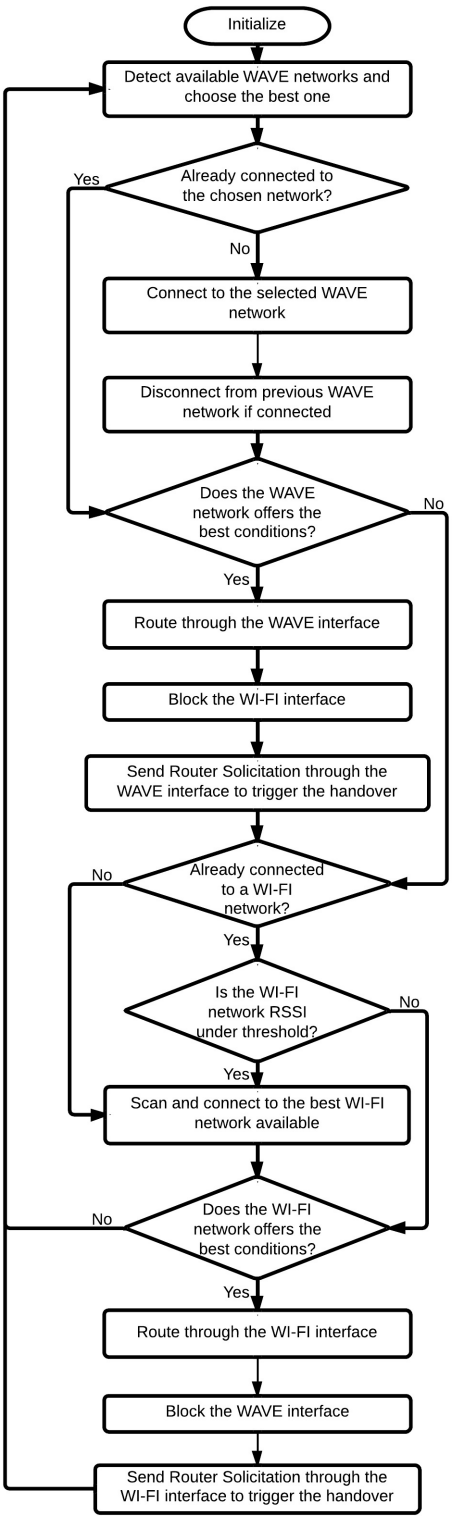


Figure 3.21: Connection manager operation flow diagram

3.8 Chapter Considerations

The need for mobility is an undeniable truth in VANETs. Both vehicles and users need to be supported when moving along the network, performing handover between the fixed infrastructures (RSUs / MAGs) or the mobile routers available (OBUs present on the vehicles / mMAGs). Not only should they be able to perform handover between access points, but also between network access technologies according to the attachment point selected. After selecting the protocol that can support all these characteristics, the N-PMIPv6 has been analyzed with respect to our requirements and its limitations, proposing solutions for the several limitations due to the novel scenarios and technologies envisaged.

After a complete study of the PMIPv6 selected implementation, it was clear the necessary changes to turn that implementation on an N-PMIPv6 implementation. However, those protocols needed to work perfectly with the specially VANET developed communication technology, the IEEE 802.11p/WAVE technology.

As the WAVE technology does not require association (in opposite to WI-FI), the broadcast messages have a different behavior from the expected, since the protocol messages like the RS/RA or NS/NA have been implemented based on the assumption that both nodes were associated. Therefore, these messages needed to be adapted as well as the mobility protocol in order to overcome these problems.

The implementation of the N-PMIPv6 protocol required modifications to the PMIPv6 code used as basis: the most significant was the implementation of the mMAG which required changes on the PMIPv6 MAG, in order to detach it from its fixed role on the protocol allowing the network mobility and also chaining mMAGs to extend the range of the connection to the Internet.

However, as the great majority of the personal devices are only IPv4 compatible, it is needed to grant their access to the Internet, even over the IPv6 vehicular network. For this purpose, it was implemented a tunneling and NAPT system capable of providing IPv4 Internet to the users connected to the vehicles, which have IPv6 connection, and which mobility is supported by the protocol implemented. These users can also share the vehicle mobility as long as they are connected to it, and therefore, they have partial IPv4 mobility.

With a working implementation of the network mobility protocol, it was still needed to implement a connection manager capable of triggering the mobile nodes handover between the available networks to keep the connection as good as possible. This module runs, together with the mobility protocol, in every mMAG, and together they provide the mobility support required to achieve the objectives of this Dissertation.

Although neither of the modules developed are valid until they are tested in real testbeds

which represent the scenarios of interest, in the next chapter we will describe the testbeds designed to evaluate the mobility protocol and we will present the obtained results, both in lab and real roads.

Chapter 4

Evaluation of the Mobility Approach

4.1 Introduction

After developing the network mobility protocol and all the necessary mechanisms, in order to be able to perform seamless mobility in a vehicular environment, it is important to analyze its performance. Our aim is to evaluate the handover process between access points that can transmit in the IEEE 802.11g or IEEE 802.11p or both. With the proper operation of the mobility protocol, it is also expected that the mobile MAG (mMAG) entities, which represent vehicles, be capable of sharing an IPv4 network that allows access to the Internet, which will also be evaluated. This chapter will therefore present the necessary mechanisms to make this assessment and analyze its outcome. The mobility to and from cellular networks is also supported. However, since it provides direct connection to the Base Station, it is not a relevant scenario from the network mobility point of view.

This chapter is organized as follows. Section 4.2 will describe the testbeds used to evaluate the performance of the mobility protocol on a vehicular environment, it will then detail the entities that will compose the testbed, and the connections and configurations necessary in each one.

Section 4.3 describes the metrics to be obtained in order to characterize the handover process, and also the methodology used to obtain these metrics. With these metrics, it will be possible to evaluate the correct implementation of the N-PMIPv6 protocol, and it will also allow to draw some conclusions about which is the access technology that better supports network mobility, the IEEE 802.11p or the IEEE 802.11g.

Section 4.4 presents the results obtained from each of the testbeds detailed on the section 4.2 for each of the different handover cases, in the lab experiments.

Section 4.5 presents the results obtained from each of the testbeds detailed on the sec-

tion 4.2 for each of the different handover cases, in the real world environment experiments.

Section 4.6 will draw the main conclusions of the chapter, analyzing the results obtained from the experiments performed.

4.2 Testbed

This section describes the testbeds and the equipment used in the experiments.

4.2.1 Equipment Used

The architectures to be studied require four fundamental entities: the LMA, the MAG, the mMAG and the MNN. In the laboratory tests, a desktop with Intel i3 processor with operating system UBUNTU 12.04 was used as the LMA, and also as an authentication radius server on the lab tests. An ACER Aspire One with an Intel Atom 32 bit processor and UBUNTU 12.04 was used on the real vehicular environment tests. This entity communicates with the MAGs using the building Ethernet network on the lab tests. For the road tests, the LMA connects to the MAGs by a WI-FI connection in order to extend the distance between them.

MAGs represent the RSUs, and the mMAGs represent the vehicles. For both MAGs and mMAGs, the equipment used is the one described in section 2.3. The IEEE 802.11p of the OBUs is configured with periodic channel switching. The MNN is an ASUS laptop with Intel i3 processor with 64bit operating system UBUNTU 12.04.

For the real vehicular environment tests, it is also needed a vehicle to move along the road performing the expected handover. The vehicle chosen is a 2 seat OPEL CORSA which is a fairly common car.

4.2.2 Testbeds implemented

In order to assess the operations of N-PMIPv6 into all the scenarios described on section 3.2, two simple testbeds were assembled, and both of them are evaluated in all the possible combination of intra and inter-technology handovers. The translation table 4.1 is valid throughout this chapter.

The first testbed aims to evaluate how the mobility protocol reacts to the handover between access points which are at the same distance, in terms of hops, to the LMA; this can be compared to a vehicle moving along a road performing handover between the available RSUs or WI-FI access points granting its occupants mobility (scenario of figure

Table 4.1: Technology Handover Cases

Name	Handover Case
P2P	IEEE 802.11p to IEEE 802.11p
P2G	IEEE 802.11p to IEEE 802.11g
G2P	IEEE 802.11g to IEEE 802.11p
G2G	IEEE 802.11g to IEEE 802.11g
G2G WS	IEEE 802.11g to IEEE 802.11g with previous scan
G2G W/O S	IEEE 802.11g to IEEE 802.11g without previous scan

3.1 and figure 3.2).

For the lab version, figure 4.1, the LMA connects to the MAG by the wired network of the building, automatically acquiring its IPv6 addresses. The LMA must be running the Radius server and the N-PMIPv6 program with a configuration file correspondent to the desired entity. The MAGs/RSUs shall be running the N-PMIPv6 protocol with a configuration file indicating that this is a MAG, assigning it a fixed address, and with a broadcasted WI-FI network or/and a WAVE provider. The mMAG configures all the wireless interfaces, WI-FI broadcast and WAVE provider, starts the connection manager program, and then the N-PMIPv6 program with the configuration file indicating that it is a MAG entity but without assigning it any address. The MNN only has to connect to the mMAG hotspot as it does in any regular WI-FI hotspot.

In the road version of the test, figure 4.2, to increase the distance between the MAGs, their communication towards the LMA is performed by a WI-FI connection. After the LMA starts, the radius and N-PMIPv6 program need to configure and broadcast a WI-FI network. In the MAGs, prior to their configuration, it needs to be established the connection to the LMA WI-FI network in order to enable their communication. After that, all the configurations proceed as normal.

The second testbed, lab version on figure 4.3 and real vehicular environment version on figure 4.4, aims to evaluate how the mobility protocol reacts to the handover between access points which are at a different number of connections from the LMA. This can be compared to a vehicle moving along a road performing handover between the available RSUs or WI-FI access points, but also between other vehicles which are extending the range of those fixed infrastructures connection granting its occupants mobility (scenario of figure 3.3 and figure 3.4).

In this testbed, all the configurations are done the same way as on testbed 1 except for

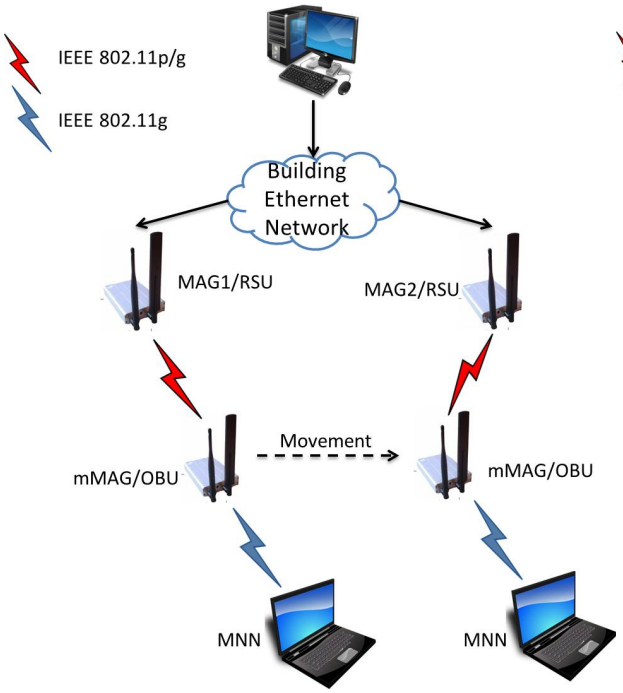


Figure 4.1: In Lab Testbed 1

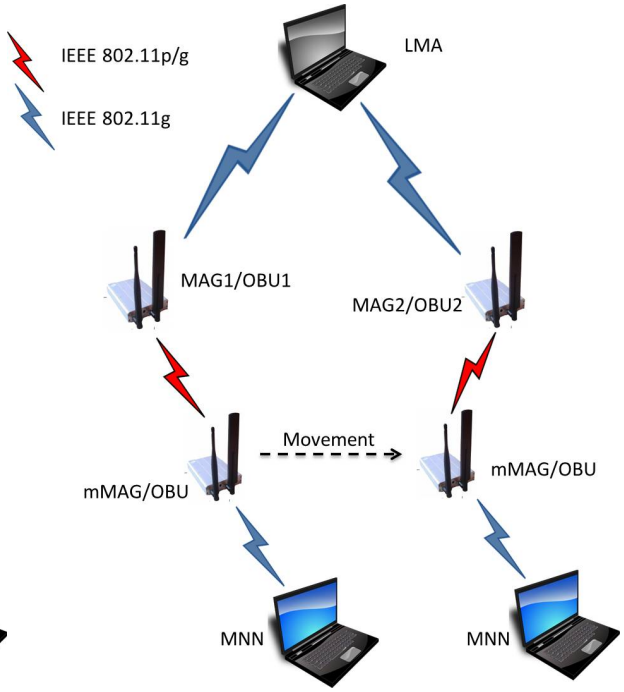


Figure 4.2: Real Scenario Testbed 1

the mMAG2 that, prior to start the N-PMIPv6 program, it has to establish a connection with MAG2 using the WAVE interface, and after that, it shall start broadcasting its own WI-FI network and WAVE provider. Finally, it has to run the N-PMIPv6 protocol with the appropriate configuration file.

The real vehicular environment tests were performed on a straight public road and the RSUs were placed right by the side of the road, as can be observed in figures 4.5 and 4.6. The vehicle was equipped with an OBU and the necessary antennas, as is depicted in figure 4.7.

In order to validate whether it is possible to spread an IEEE 802.11g IPv4 network on the OBU that allows users within the vehicle to access to the Internet, it is implemented the testbed of Figure 4.1 in a lab environment, but the IEEE 802.11g connection between the mMAG and MNN is now IPv4 instead of IPv6. With this approach, the MNN can access the IPv4 Internet through its connection to the mMAG, even while it performs handover between different access points.

4.3 Methodologies and metrics

In this section we define the metrics to be obtained. They are the following:

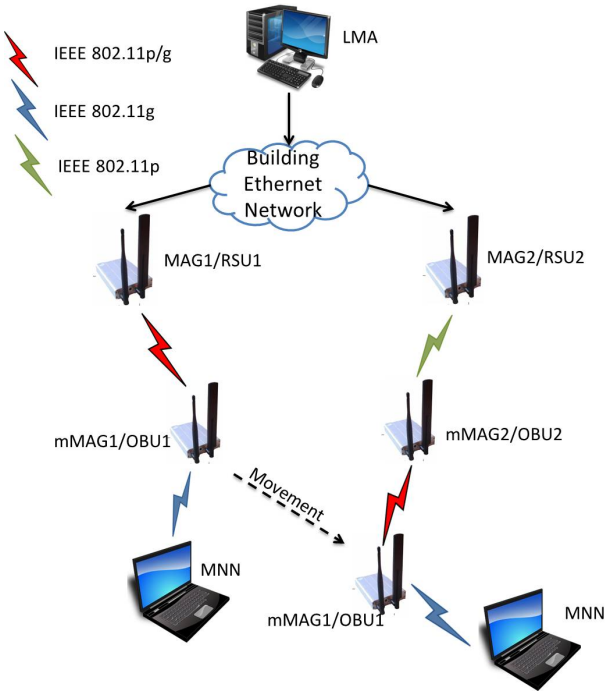


Figure 4.3: In Lab Testbed 2

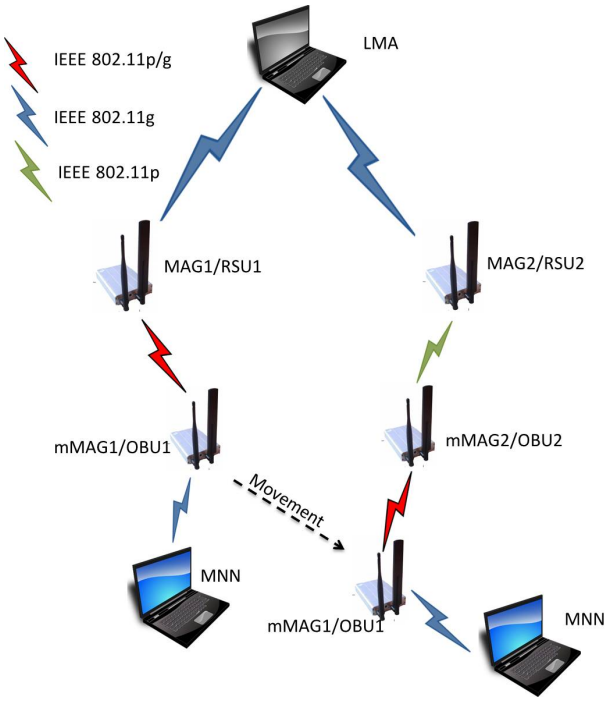


Figure 4.4: Real Scenario Testbed 2

- Lag time of the handover process.
- Average number of lost packets during the handover process.
- Throughput before, during and after the handover procedure.
- Jitter before, during and after the handover procedure.

Through this set of metrics it is possible to get a good characterization of the handover process. The latency of the handover process will be one of the most important, because it defines more precisely the time interval in which there is loss of connection when the node moves from one network to another. The average number of packets lost, the troughput and the jitter allow to take conclusions on the effect of the handover process on the Quality of Service (QoS) offered to users. Based on these metrics, it is also possible to take conclusions on the behavior of each technology for the handover process and determin which one is more suitable for use in vehicular environments.

To obtain the necessary metrics it was necessary to generate traffic between the CN and the MNN (or mMAG depending on the scenario). The desktop where the LMA is running is also used as a CN. To generate traffic, it is used the *Iperf* tool [44]. This tool allows generating traffic using the transport protocols Transmission Control Protocol (TCP) or

Figure 4.5: RSU 1

Figure 4.6: RSU 2 / OBU 2

User Datagram Protocol (UDP). To carry out the testing, only UDP traffic was generated because with this protocol there are no retransmissions which will allow getting the wanted metrics with greater reliability. This program immediately provides three of the metrics that will be evaluated; the average number of lost packets, jitter and the throughput.

To obtain data about the handover latency, it is used a tool called *Tshark* to capture information about the packets sent from the CN and then received on MNN / mMAG. With this information, subtracting the time of the first packet received through the new network to the time of the last packet received through the old network, it is obtained the latency of the handover process.

To analyze the metrics, two *python* programs were used to process the outputs of the tools *Tshark* and *Iperf* which were then processed in a MATLAB script [22] in order to

Figure 4.7: OBU / Vehicle

obtain the graphs.

These results were obtained from a minimum of 5 repetitions of each of the tests, and the confidence intervals shown are of 95%.

To make the evaluation of the ability of mMAG spread the IPv4 network providing access to the Internet, a video will be recorded showing the screen output of the MNN while it accesses to the Internet, in order to assess whether there is loss of connection or session when mMAG performs handover between different access points.

4.4 Lab Experiments Results

The results obtained from the lab experiments will now be presented. The tests were carried out on three different traffic speeds, 256Kbit/s, 512Kbit/s and 1Mbit/s and every bar graphics are in that order for each handover case. In the figure with time in the x-axis, the handover initiates on the moment signalized by the vertical black line.

All the graphics shown on this section have been regulated in order to adjust the handover procedure starting point to be at the same instant in all the graphics allowing an

easier comparison between the tests performed. The handover moment was detected using the *Tshark* script identifying when the route followed by the packets has changed. The results were then displayed around that point. As the jitter is only significantly affected at the handover instant, the jitter graphics were centered on that exact instant.

4.4.1 Results obtained through the testbed 1

Handover Latency

Figure 4.8 and figure 4.9 show the latency of the handover process between technologies in handovers between access points with the same number of hops to the LMA. It is clear that the IEEE 802.11g technology is not a mobility prepared technology for these environments, since it takes a longer time to perform the handover. As the mMAG shares the IEEE 802.11g interface with the network to which it is connected (input network), and also with the network that it broadcasts into the vehicle (output network), it even makes the process worse. This is because the scan procedure of the input network blocks the interface, which means that the output network will be momentarily without connection. This translates in a larger packet loss in any handover procedure between an IEEE 802.11g, as can be shown in figure 4.10. Notice that inter-technology handovers or handovers between IEEE 802.11p do not have losses. If the handover is forced, it is then possible to perform the handover to an IEEE 802.11g network without doing a scan first, and therefore, reducing the connection lost time. As can be seen in figure 4.8, the handover latency between IEEE 802.11g networks is larger when the scan is active than when it is inactive. With respect to the other handover cases, the best scenario is between IEEE 802.11p networks or from an IEEE 802.11g to an IEEE 802.11p network, since it does not require performing any scan on the IEEE 802.11g interface.

Throughput and Packet Loss

The same problem about the IEEE 802.11g network can also be seen in the throughput results on the figure 4.11. The throughput is only affected when the handover is performed between IEEE 802.11g networks, or to an IEEE 802.11g network. However, this is not due to the mobility protocol, but it is only a limitation of the IEEE 802.11g technology. In the other cases the mobility protocol has a very good performance. The packet loss is obviously much larger in the handover cases with significant throughput variations.

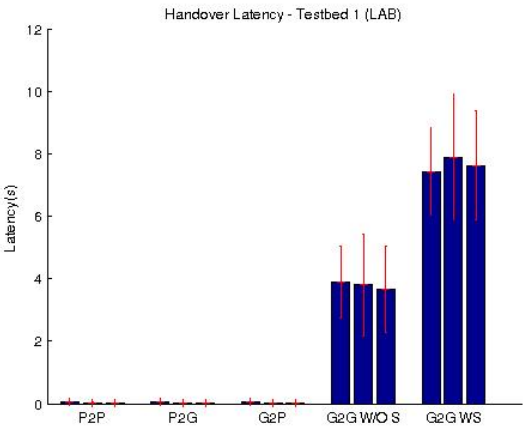


Figure 4.8: Handover Latency (tb1-lab)

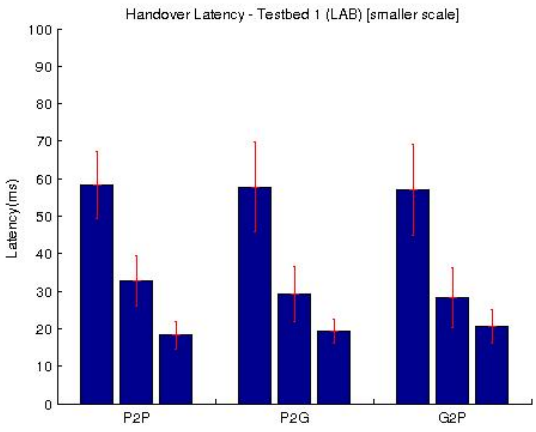


Figure 4.9: Detail of figure 4.8

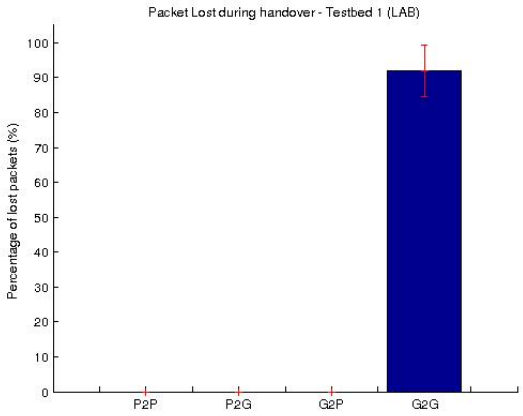


Figure 4.10: Packet Loss (tb1-lab)

Jitter

The jitter only changes when the handover occurs between different technologies as was expected since every technology as its own characteristics. The results can be seen in figure 4.12. We observe that the jitter is larger in IEEE 802.11p technology, due to the periodic channel switching of this technology.

4.4.2 Results obtained through the testbed 2

This sub-section considers the lab scenario with access points connected to LMA with a different number of hops.

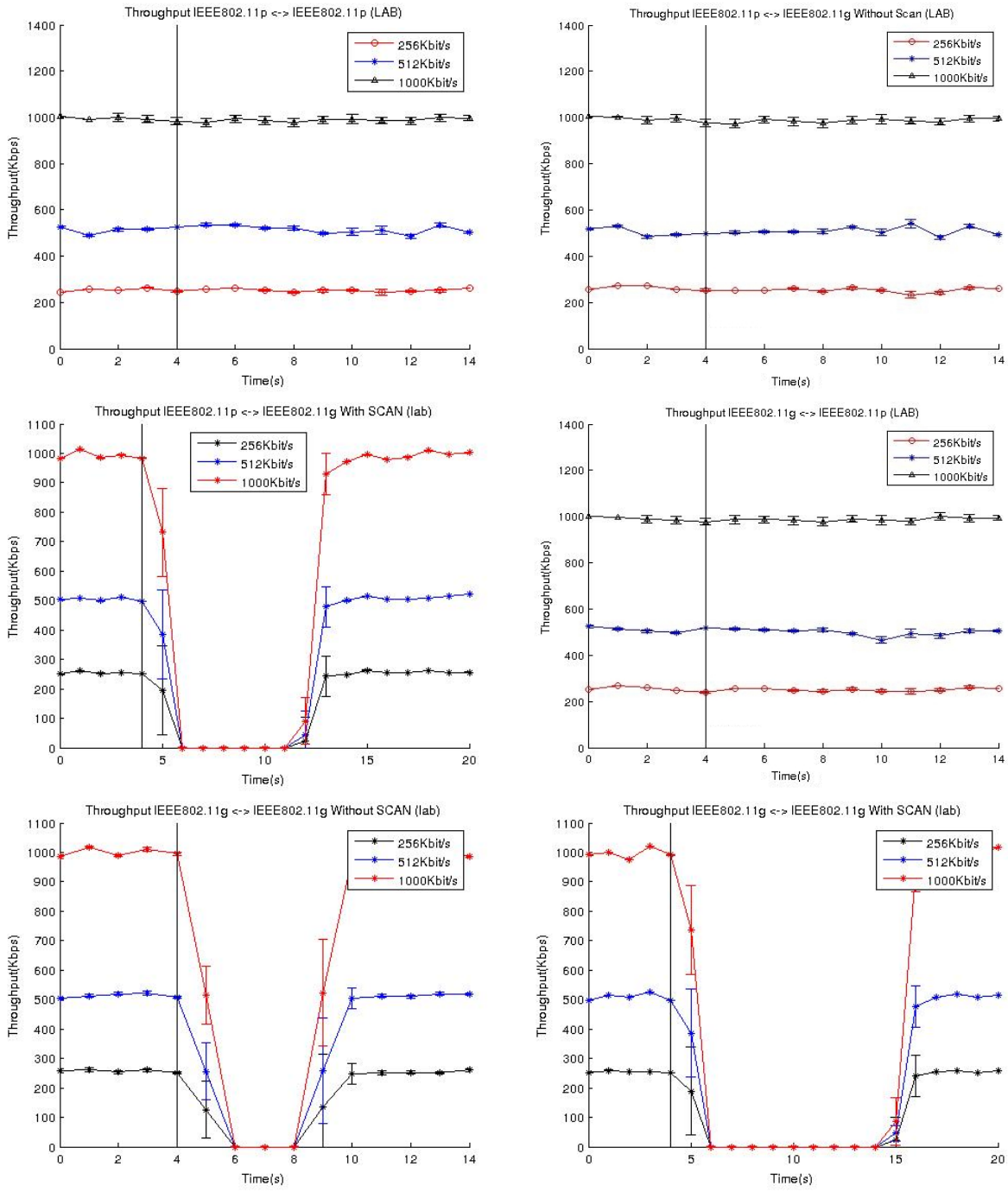


Figure 4.11: Throughput (tb1-lab)

Handover Latency

Once again comparing the latency of the handover process between technologies it is clear that the IEEE 802.11g technology keeps being the slowest one to perform handover.

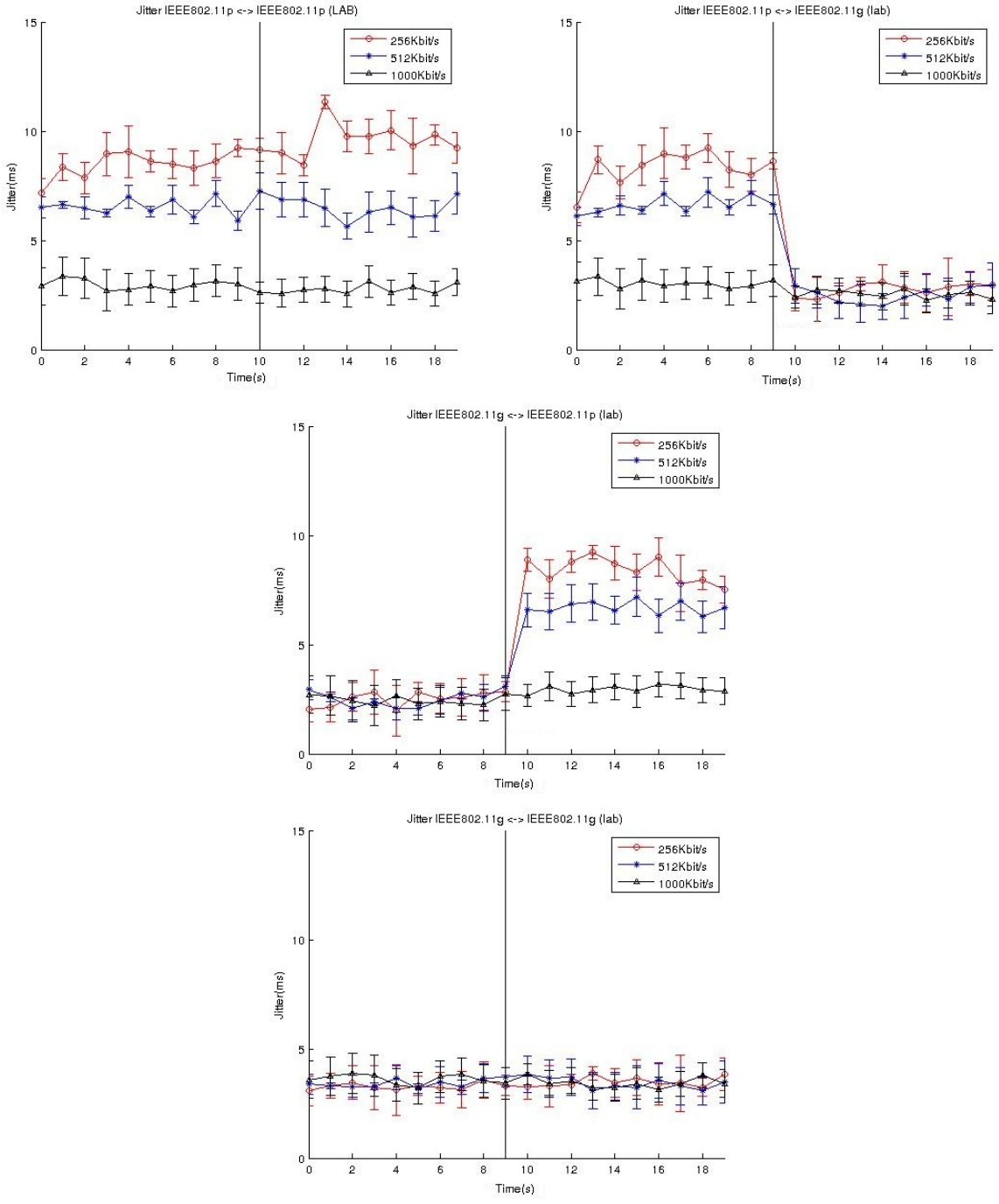


Figure 4.12: Jitter (tb1-lab)

In fact, it is expected that the latency times remain approximately the same as on the testbed 1, since the only difference is that the mobility protocol control messages only have to travel one extra link, which is not supposed to affect the protocol speed significantly.

These results can be seen in figure 4.13 and figure 4.14.

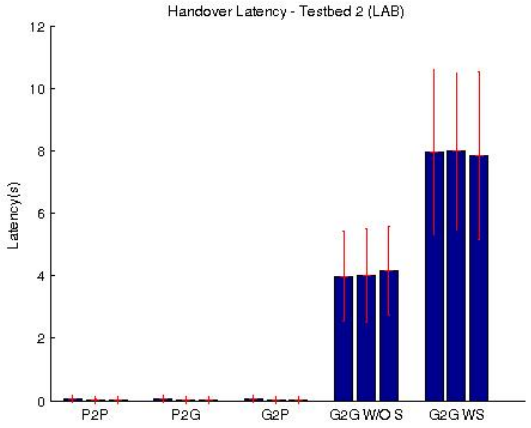


Figure 4.13: Handover Latency (tb2-lab)

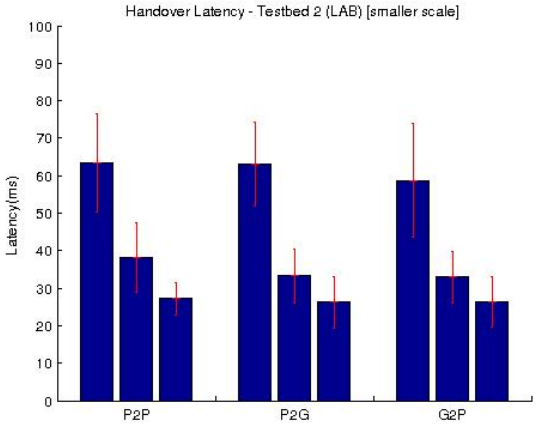


Figure 4.14: Detail of figure 4.13

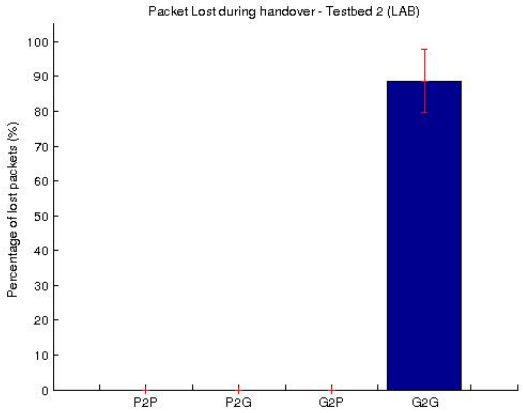


Figure 4.15: Packet Loss (tb2-lab)

Throughput and Packet Loss

The throughput (figure 4.16) and packet loss (figure 4.15) results are also very similar to the ones obtained in testbed 1, which is also expected. It is important to notice that the number of hops in a chain, in a lab environment, does not affect the data in the network mobility.

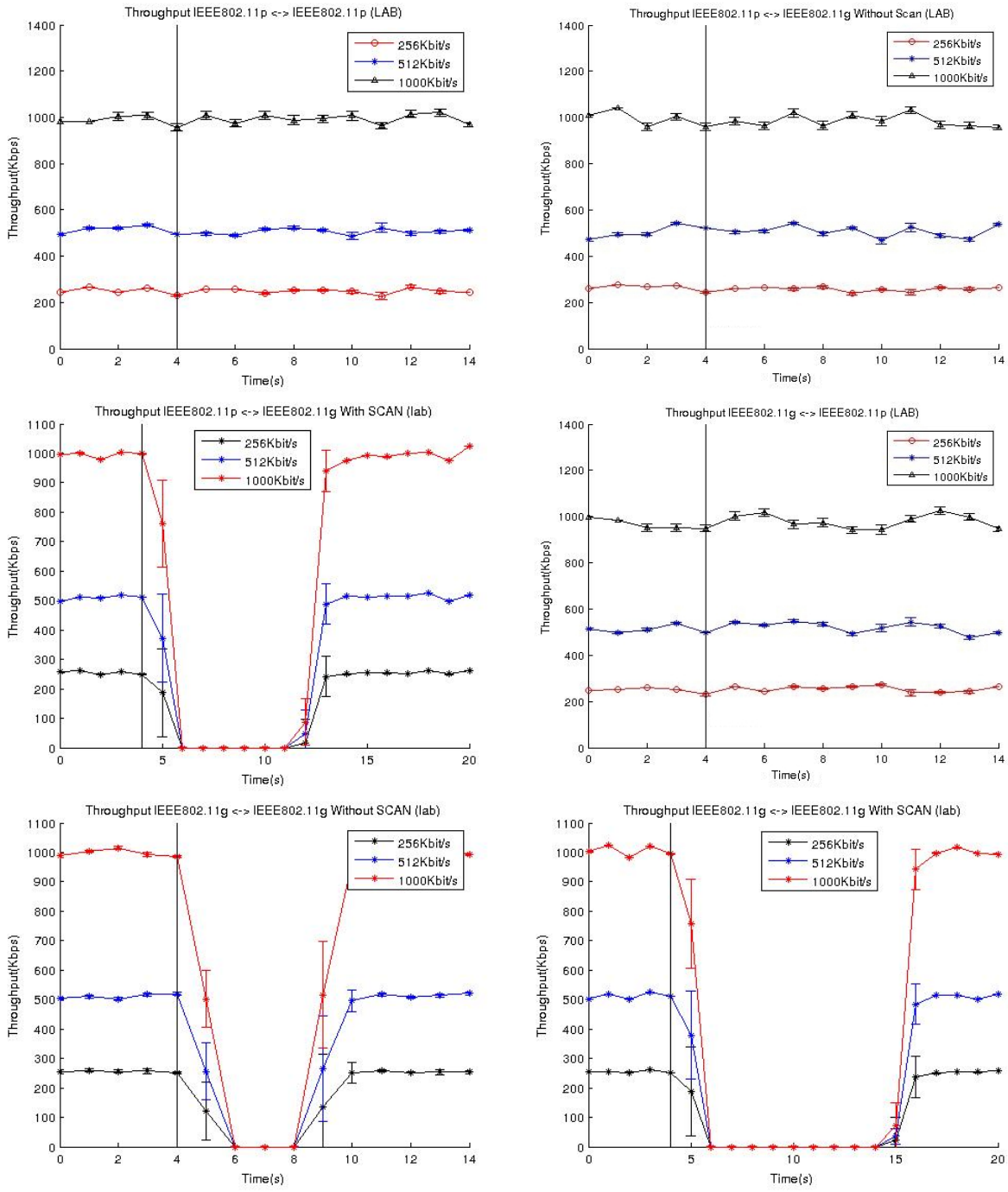


Figure 4.16: Throughput (tb2-lab)

Jitter

In this testbed, the jitter is expected to change after the handover due to the increase of the number of links that the packets have to travel. After the handover procedure, every

packet has to cross an extra IEEE 802.11p link. The results are depicted on figure 4.17.

4.4.3 Results of the IPv4 network broadcast

This section shows if it is possible to spread an IPv4 network to share Internet access in the vehicle for a regular IPv4 user. This requires a tunneling system over the IPv6 network managed by the N-PMIPv6, and a NAT system in the central entity, the LMA. To prove its correct operation, it has been performed the experiment depicted in the Figure 4.1, and the result is recorded in a video, which is available at the following URL:

https://www.youtube.com/watch?v=JTXOg1c6qV4 (figure 4.18)

In this video, it is shown that the handovers are performed while the user is watching the video from the Internet, and no problems are noticed on the video when the handover occurs. We thus show the ability of a user to obtain IPv4 Internet through the OBU in the vehicle, even when it moves between different access points, with completely seamless mobility.

4.5 Road Experiments Results

The results obtained from the tests carried out in the road will now be presented. The tests were carried out with a traffic rate of 512Kbit/s, and with the vehicle moving at a speed of approximately 70km/h. The handover procedure initiates on the moment signaled by the vertical black line. Due to the fact that the connection between the RSUs/MAGs and the LMA is now performed by a WI-FI connection, it is expected an increase of the jitter values comparing to the ones obtained in the lab tests.

All the graphics shown on this section have been regulated in order to adjust the handover procedure starting point to be at the same instant in all the graphics, allowing an easier comparing between the tests performed. The handover moment was detected using the *Tshark* script identifying when the route followed by the packets has changed. The results were then displayed around that point. As the jitter is only significantly affected at the handover instant, the jitter graphics were centered on that exact instant.

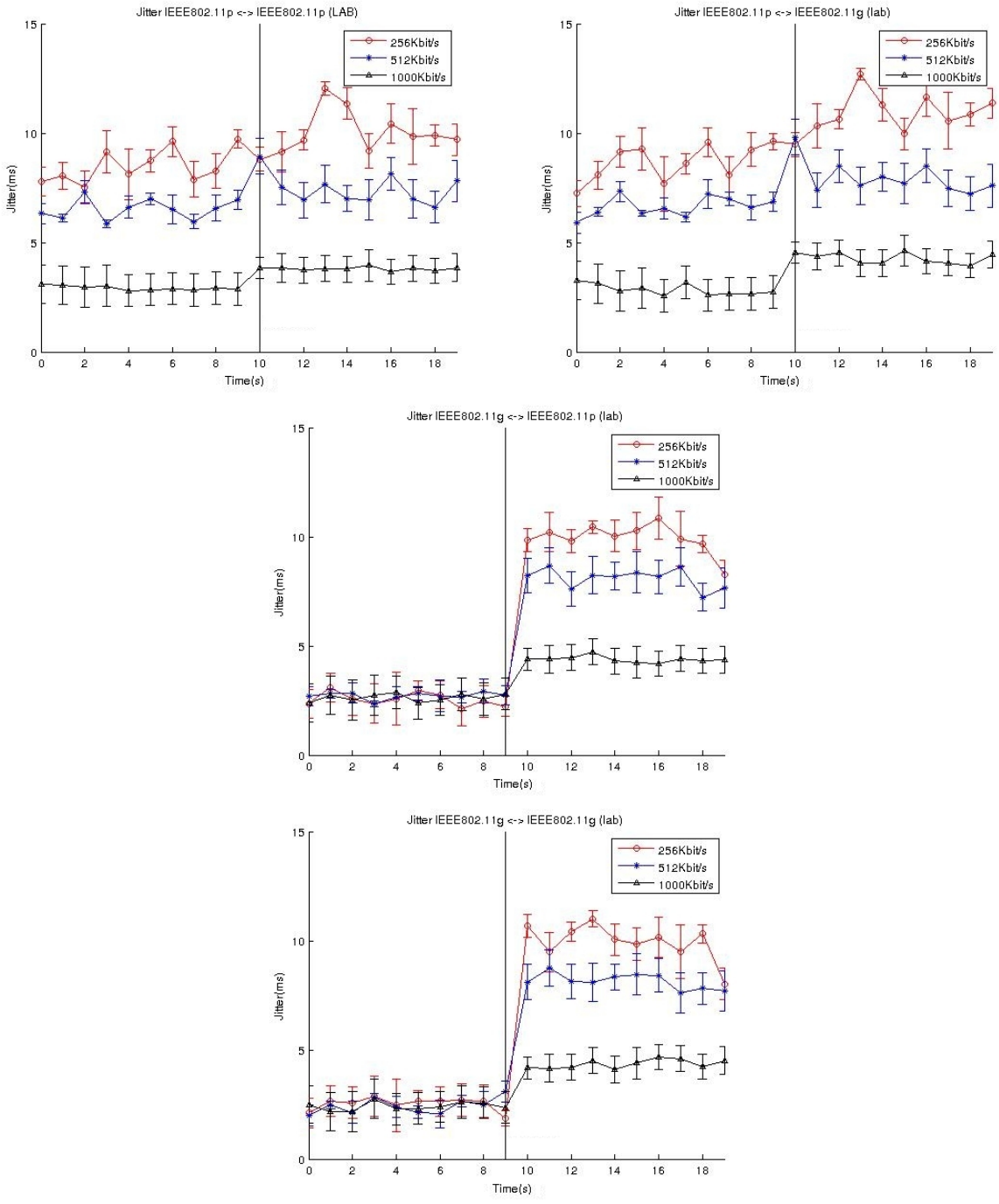


Figure 4.17: Jitter (tb2-lab)

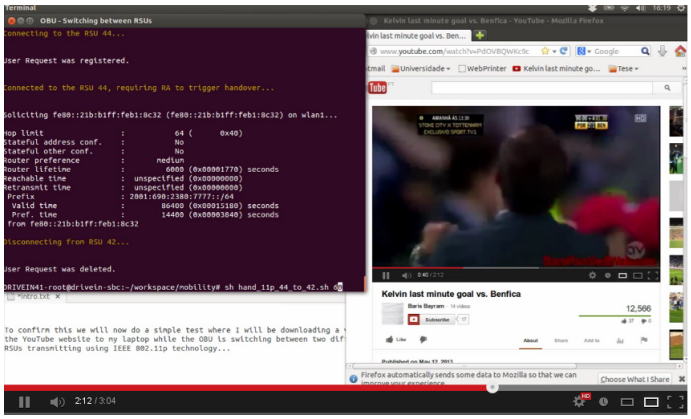


Figure 4.18: Capture from the video

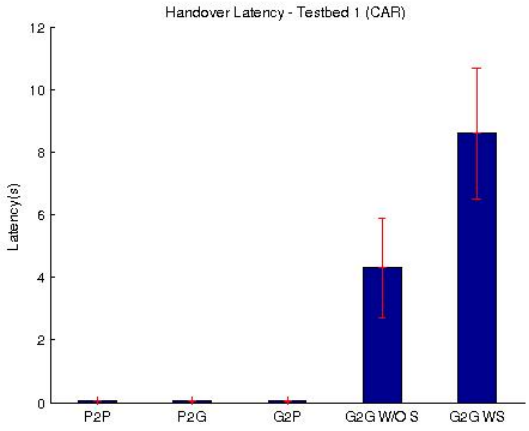


Figure 4.19: Handover Latency (tb1-road)

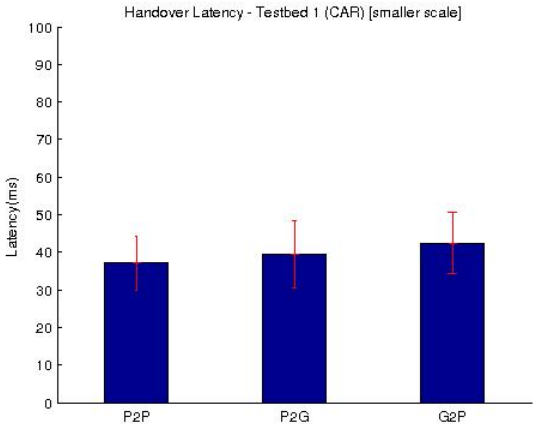


Figure 4.20: Detail of figure 4.19

4.5.1 Results obtained through the testbed 1

Handover Latency

The latency results can be seen in figure 4.19 and with better detail in figure 4.20. Comparing them with the results of the lab tests, which can be seen in figure 4.8 and 4.9, it is possible to confirm that they are very similar, and therefore, the WI-FI connection between the LMA and the MAGs does not affect significantly the handover latency values. However, the latency values are slightly higher than the ones in the lab experiments.

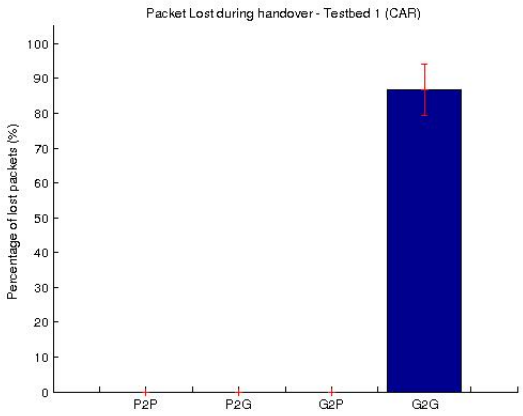


Figure 4.21: Packet Loss (tb1-road)

Throughput and Packet Loss

The throughput and packet loss results are depicted in figures 4.22 and 4.21. Comparing them with the results of the lab tests, which can be seen in figures 4.11 and 4.10, it is possible to confirm that they are very similar. Since the throughput and packet loss are not directly affected by the delay, the WI-FI connection between the LMA and the MAGs does not affect significantly these results.

Jitter

The jitter results can be observed in figure 4.23. Comparing them with the results of the lab tests, which can be seen on figure 4.12, it is possible to confirm that they are similar. However, the WI-FI connection between the LMA and the MAGs does increase the jitter values in approximately 2 to 4 milliseconds, as expected.

4.5.2 Results obtained through the testbed 2

Handover Latency

The latency results can be observed in the figure 4.24, and with greater detail in figure 4.25. Comparing them with the results of the lab tests, which can be observed in figure 4.13, it is possible to confirm that an they are very similar, and that an extra hop connecting the LMA does not influence negatively the handover delay.

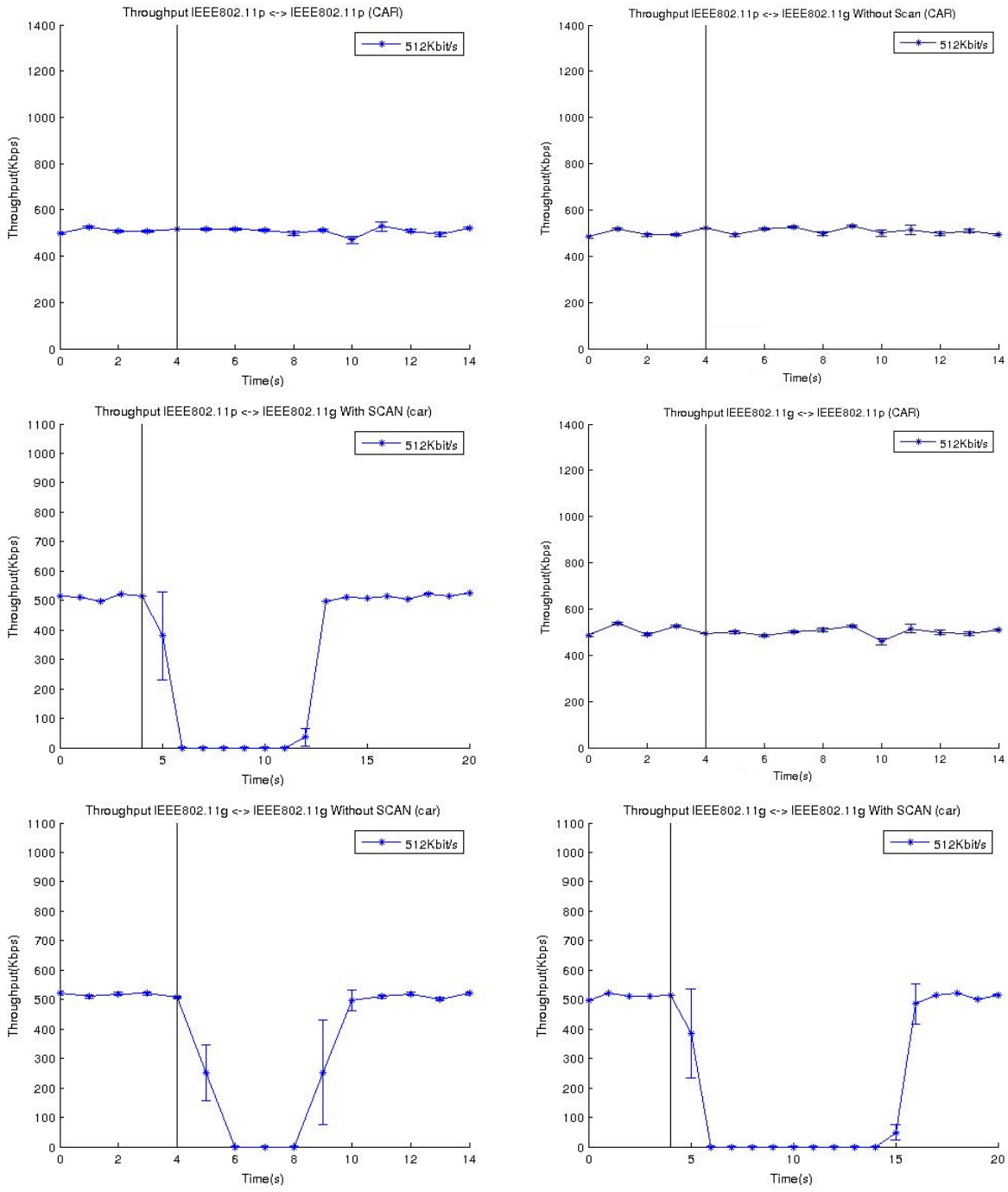


Figure 4.22: Throughput (tb1-car)

Throughput and Packet Loss

The throughput and packet loss results are depicted in the figures 4.27 and 4.26. Comparing them with the results of the lab tests, which can be seen on figure 4.16 and 4.15, it

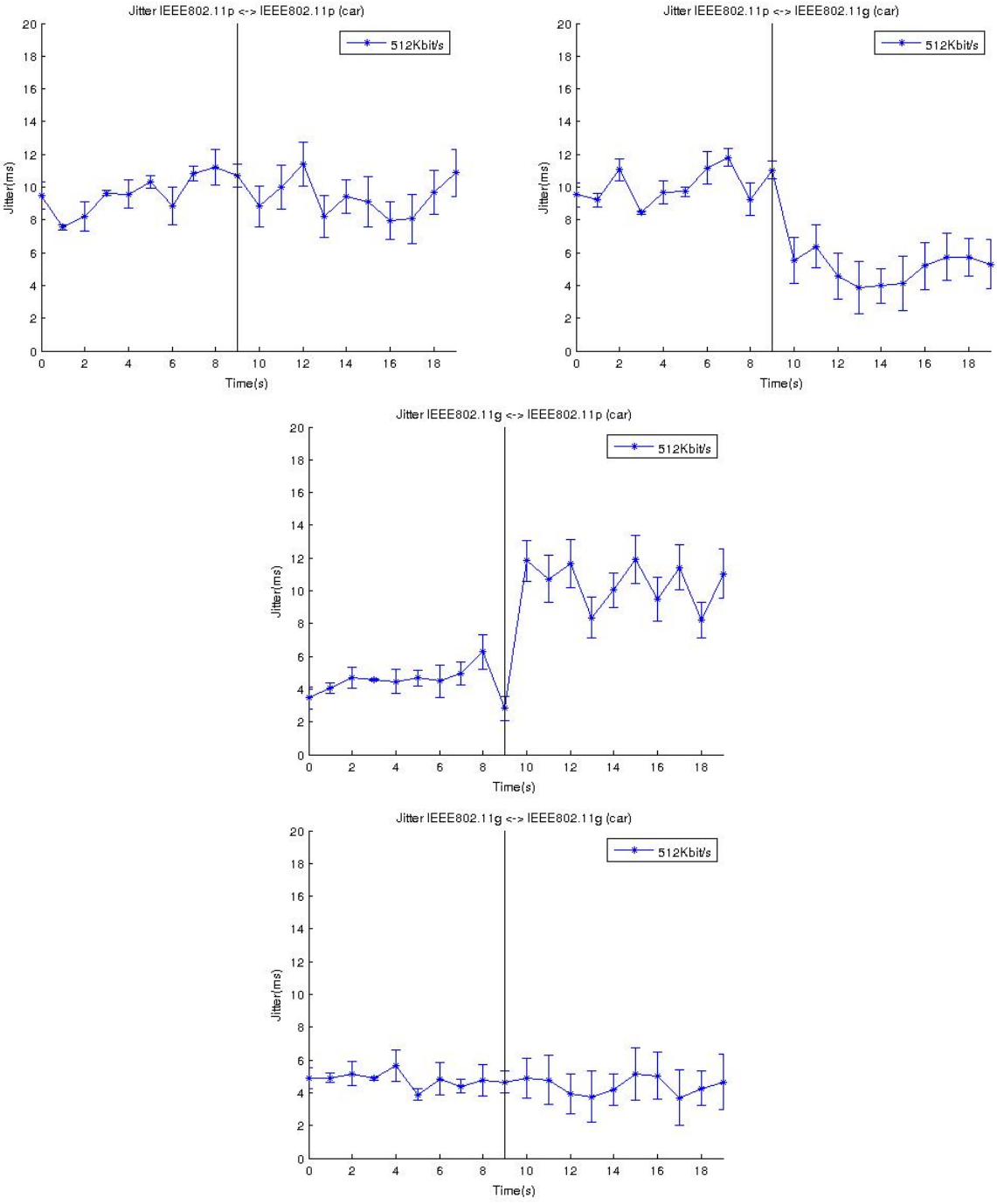


Figure 4.23: Jitter (tb1-car)

is possible to confirm that they are again very similar, and are not affected by the extra hop connecting to the LMA.

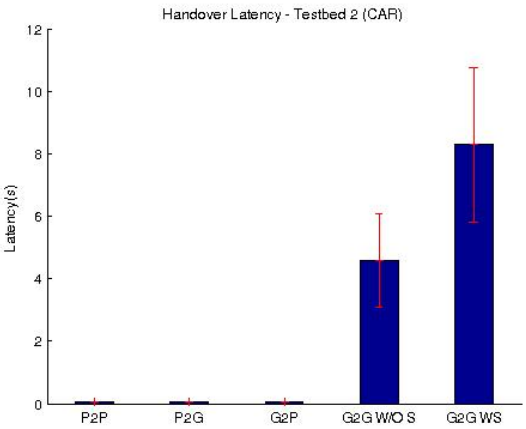


Figure 4.24: Handover Latency (tb2-road)

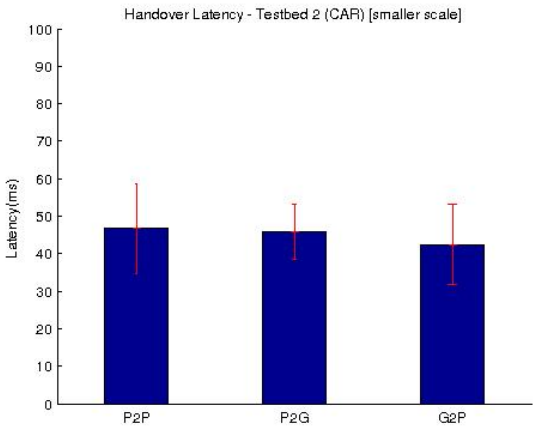


Figure 4.25: Detail of figure 4.24

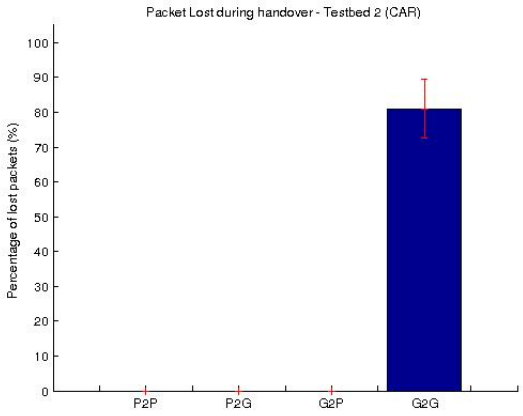


Figure 4.26: Packet Loss (tb2-road)

Jitter

The jitter results can be observed in figure 4.28. Comparing them with the results of the lab tests, which can be seen on figure 4.17, it is possible to confirm that they are again similar; however, there is a little jitter increase, which is due to the WI-FI connection between the LMA and the MAGs.

4.6 Chapter Considerations

The results obtained through the tests performed in the implemented testbeds allow to draw some conclusions about the validity of the mechanisms developed.

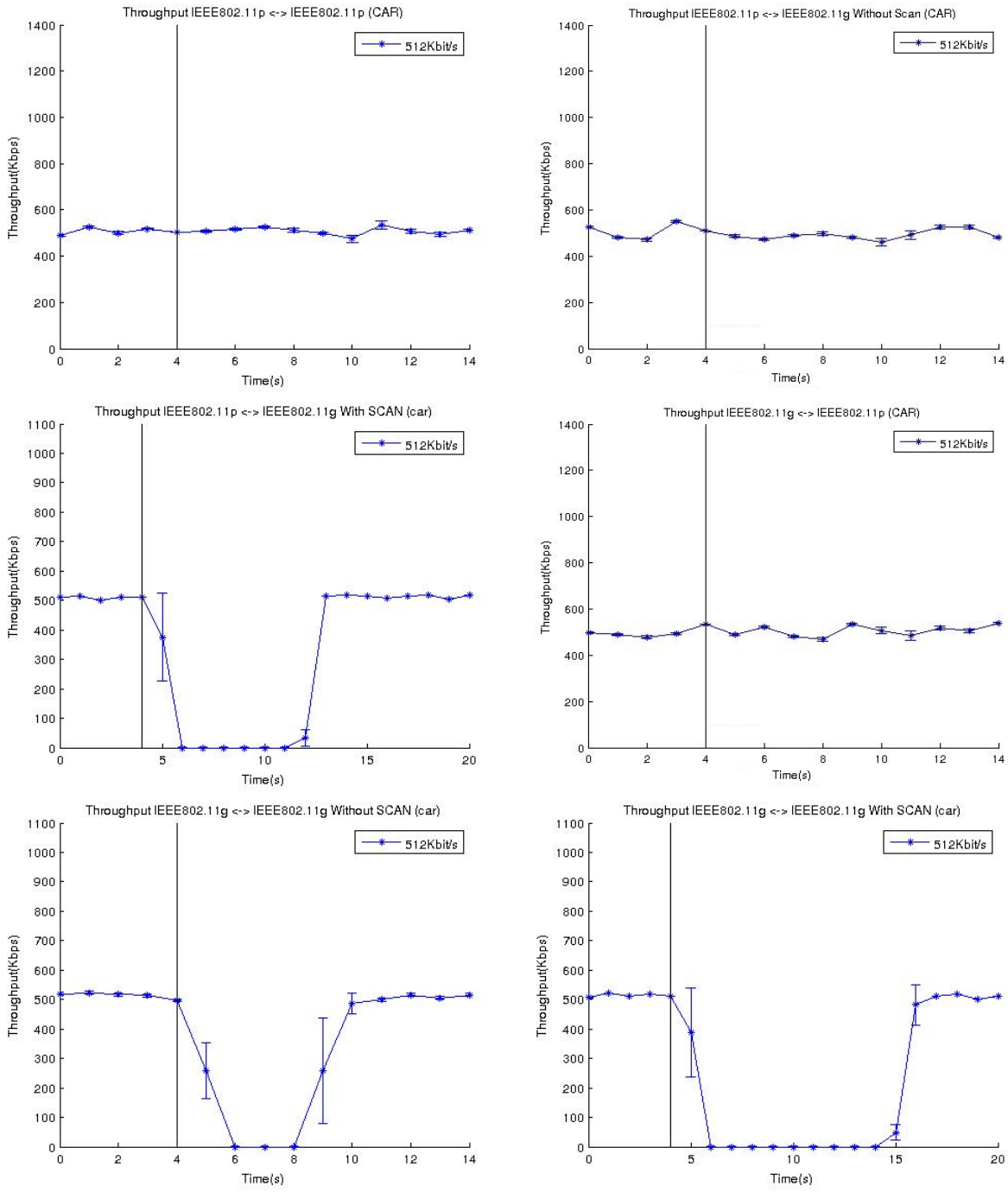


Figure 4.27: Throughput (tb2-car)

The results of the testbed 1 in a lab scenario have shown the correct operation of the mobility protocol, since it was able to support the mMAG mobility through different attachment points, as well as for the mMAGs sub-network. It has also been shown the

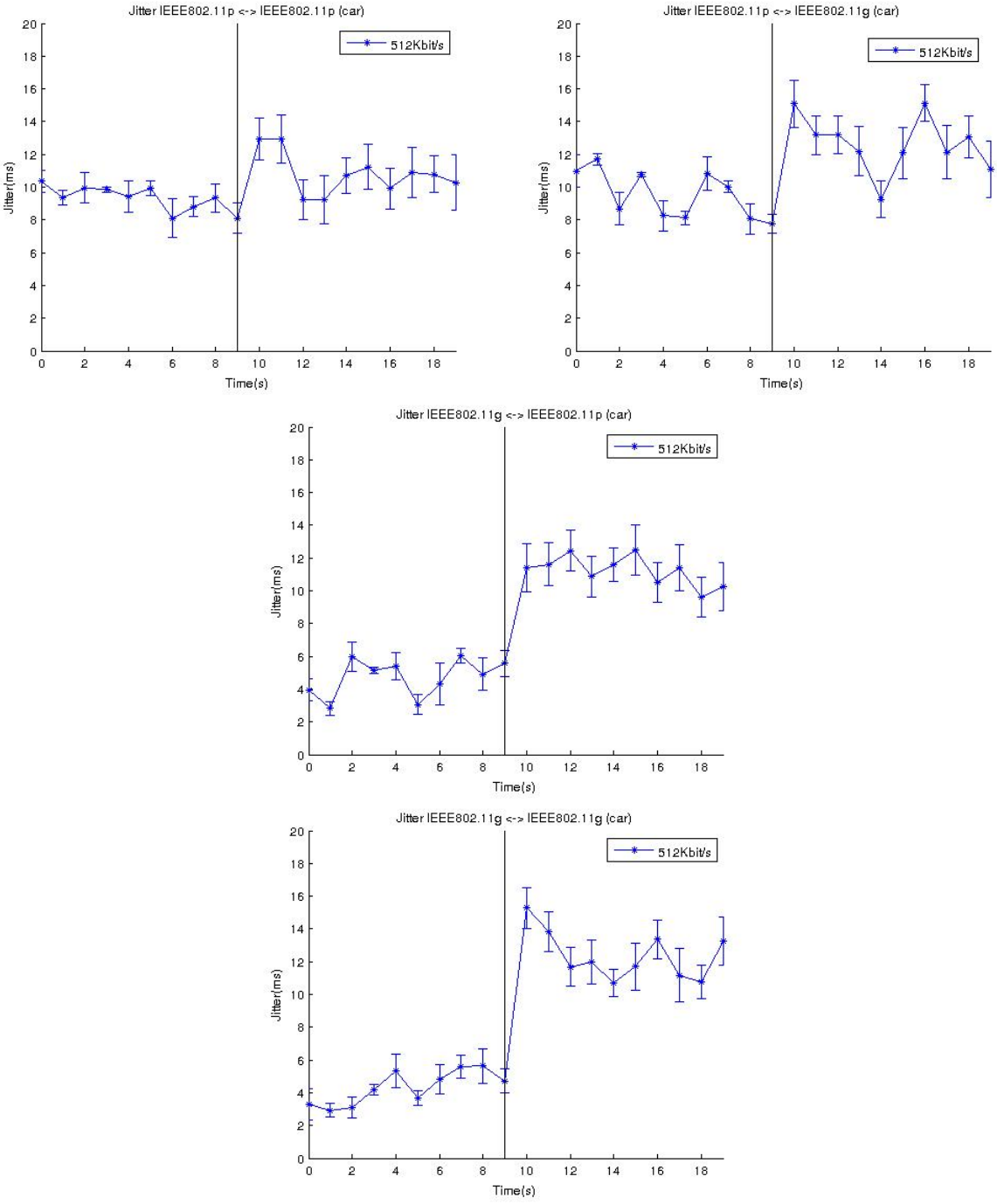


Figure 4.28: Jitter (tb2-car)

capacity of the mobility protocol to support handover not only between attachment points of the same technology but also between different technologies.

However, IEEE 802.11g is not prepared for mobility which reflects in higher handover

latency values and higher packet losses due the connection interruption. The IEEE 802.11g affects severely the mobility protocol performance. This problem has also been worsened by the fact that the mMAG shares the IEEE 802.11g interface between the connection from which it receives traffic and the connection that it broadcasts to its users. Since to perform mobility to an IEEE 802.11g network, it is needed to perform a scan on that interface to evaluate the available networks, it gets blocked during that scan process. This means that, in every handover performed to an IEEE 802.11g with a scan procedure, it will result in the loss of packets due the broadcasted network interruption. In figure 4.11, it can be observed the difference on the throughput values when the scan is or not active.

In the remaining cases, i.e., when the handover is performed to an IEEE 802.11p network, the throughput remains approximately constant which translates in a low (or even none) packet loss.

The results of the testbed 1 in a real vehicular environment, section 4.4.1, have demonstrated the validity of the laboratory results, since the road results are very similar to the lab ones.

The results of the testbed 2 in a lab environment showed the ability of the N-PMIPv6 to support network mobility between attachment points at a different number of hops from the LMA. This will allow the mMAGs to extend the RSUs connection range by acting like repeaters, and therefore, reducing the need of fixed infrastructures. The results of testbed 2 on a vehicular environment have proven the validity of the lab results.

It is also visible the way the handover between attachment points at a different number of hops from the LMA affects the jitter. The jitter may be highly increased or decreased depending if the car moves from a lower attachment point to a higher attachment point or the opposite, and this is also affected by the link technologies involved, not only between the mMAG and his attachment point, but also between that attachment point and its own attachment point; the larger the chain, the most can fluctuate the jitter value.

Chapter 5

Conclusions and Future Work

5.1 Conclusions

The work developed in this Dissertation aimed to develop a mobility protocol capable of supporting the movement of a complete network. Along with this protocol it was necessary to develop a connection manager that can automate the process of finding and connecting to the best available access point in order to maintain the highest quality connection possible. To make real use of vehicular networks, as there is still a little number of applications specifically developed for these, it was necessary to implement methods to allow users to access IPv4 Internet through IPv4 WI-FI network inside the car, and support their mobility such as the network moves with the vehicle.

In order to meet these objectives, it was necessary to proceed with the following implementations: the implementation of Protocol N-PMIPv6, which is an extension of PMIPv6 mobility protocol to extend the mobility to the entire network; the implementation of the connection manager, a module that aims to monitor, select and connect the node to the best network available; the extension of N-PMIPv6 to work with broadcast networks without association, such as IEEE 802.11p; and finally, the tunneling system that will allow the OBUs to provide IPv4 Internet to the users within, who can easily access it via a smartphone or tablet, like in a regular hotspot.

To validate the correct operation of the various mechanisms developed, both lab and road tests were performed, which allowed to evaluate, according to the chosen metrics, the performance of the mobility protocol adopted to vehicular networks, and supporting network mobility.

From the results shown in Chapter 4 we can take the following conclusions:

- The VANET N-PMIPv6 mobility protocol is indeed capable of supporting the mo-

bility of each node individually and also of an entire network.

- The VANET N-PMIPv6 shows values of throughput, latency and jitter similar to the protocol which it is based, the PMIPv6, whose functioning was previous evaluated in [11].

- The handover between access points with IEEE 802.11p introduces handover latency in the order of a few milliseconds with throughputs up to 1MB/s and no packet loss (Figure 4.11 and 4.10). Moreover, if the handover is made between access points connected to the LMA through a different number of hops, the jitter keeps the same values (Figure 4.12), as well as the other metrics.

- In the case of inter-technology handover there is also a low handover latency and therefore, no packets are lost for the throughput values measured.

- The handover between access points with IEEE 802.11g revealed itself as the worst case of handover latency, as it takes between 4 to 8 seconds which leads to a loss of connection and consequent loss of packets (Figure 4.10). It is further noted that the jitter associated to this technology tends to have higher values, as the mobile MAG (mMAG) moves to a network at a higher number of hops.

- The use of virtual interfaces to try to overcome the issues of the IEEE 802.11g proved itself insufficient, since it results in large packet loss values between any handover case to an IEEE 802.11g, even if the previous network was a IEEE 802.11p network.

- The proposed approach has the ability of the mobile nodes to access IPv4 Internet, while being supported by the mobility of its access point (the mMAG), so there is no loss of connection or session even in situations of mMAG handover.

From these results we conclude that the technology that best suits vehicular networks is the IEEE 802.11p, since it presents better behavior during handover situations in addition to being a network of larger range. On the other hand, the IEEE 802.11g presents serious problems, such as loss of connection and highly variable jitter which could only be smoothed if another interface of this technology is added.

We can conclude that the developed protocol is suitable for the expected types of scenarios, and along with the IPv4 access system, it allows users to seamlessly take advantage of the vehicular networks.

5.2 Future work

Throughout the Dissertation, it was possible to detect that there are still gaps that need to be improved or developed. Noteworthy:

- `The limitations of the IEEE 802.11g technology`: despite the fact that this technology is not designed for mobility in vehicular networks, it is indeed an excellent source of fixed stations, as there are thousands of WI-FI hotspots already installed in the cities. It is important to develop methods to allow better results with this technology.

- `The mobility protocol increases the overhead in the network`: despite the fact that the N-PMIPv6 mobility protocol works properly in vehicular networks, this introduces an overhead which will be as higher as the number of hops, what may ultimately create problems for network scalability. Then an alternative with better performance shall be analyzed.

- `Evaluation of the protocol on real world uncontrolled scenarios`: evaluate the performance of the protocol in a real uncontrolled vehicular network, equipping the installed OBUs and RSUs with the mobility protocol.

- `Evaluation of the protocol with real world Access Points`: evaluate how the protocol reacts with real world IPv4 non-customized WI-FI access points, such as ZON-FON or PT-WI-FI, and analyze the changes to the protocol to make it work through those access points.

- `Integration with the advanced connection manager`: this has been developed in a parallel MSc Dissertation in the same research group, and makes use of advanced mechanisms to detect which is the best network available based not only on the RSSI of the signal, but also on the vehicles direction and speed improving the efficiency of the handover procedure.

Bibliography

[1] Ndisc6 : Ipv6 diagnostic tools for linux and bsd. *Available: http://www.remlab.net/ndisc6/*, 2013.

[2] Waleed Alasmary and Weihua Zhuang. Mobility impact in ieee 802.11 p infrastructureless vehicular networks. *Ad Hoc Networks*, 10(2):222–230, 2012.

[3] Carlos Ameixieira, José Matos, Ricardo Moreira, André Cardote, Arnaldo Oliveira, and Susana Sargento. An ieee 802.11 p/wave implementation with synchronous channel switching for seamless dual-channel access (poster). In *Vehicular Networking Conference (VNC), 2011 IEEE*, pages 214–221. IEEE, 2011.

[4] Marc Blanchet et al. Special-use ipv6 addresses. IETF RFC 5156, April 2008.

[5] Perkins Calhoun and Charles Perkins. Mobile ip network access identifier extension for ipv4. Technical report, IETF RFC 2794, March, 2000.

[6] Yuh-Shyan Chen, Ching-Hsueh Cheng, Chih-Shun Hsu, and Ge-Ming Chiu. Network mobility protocol for vehicular ad hoc networks. In *Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE*, pages 1–6. IEEE, 2009.

[7] Lin Cheng, Benjamin E Henty, Reginald Cooper, Daniel D Stancil, and Fan Bai. A measurement study of time-scaled 802.11 a waveforms over the mobile-to-mobile vehicular channel at 5.9 ghz. *Communications Magazine, IEEE*, 46(5):84–91, 2008.

[8] Imrich Chlamtac, Marco Conti, and Jennifer J-N Liu. Mobile ad hoc networking: imperatives and challenges. *Ad Hoc Networks*, 1(1):13–64, 2003.

[9] Juliusz Chroboczek et al. The babel routing protocol. IETF RFC 6126, April 2011.

[10] Thomas Clausen, Philippe Jacquet, Cédric Adjih, Anis Laouiti, Pascale Minet, Paul Muhlethaler, Amir Qayyum, and Laurent Viennot. Optimized Link State Routing

Protocol (OLSR), 2003. HIPERCOM - INRIA Rocquencourt , Département Logiciels et Réseaux - LOR , GANG - INRIA Rocquencourt, Network Working Group.

[11] Jorge Dias, André Cardote, Filipe Neves, Susana Sargento, and Arnaldo Oliveira. Seamless horizontal and vertical mobility in vanet. In *Vehicular Networking Conference (VNC), 2012 IEEE*, pages 226–233. IEEE, 2012.

[12] Yingtian Du, Lin Zhang, Yufei Feng, Zhanyang Ren, and Zi Wang. Performance analysis and enhancement of ieee 802.11 p/1609 protocol family in vehicular environments. In *Intelligent Transportation Systems (ITSC), 2010 13th International IEEE Conference on*, pages 1085–1090. IEEE, 2010.

[13] K. Fall e K. Varadhan. The network simulator ns-2. *Available: http://www.isi.edu/nsnam/ns*, 2013.

[14] Stephan Eichler et al. Performance evaluation of the ieee 802.11 p wave communication standard. In *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, pages 2199–2203. IEEE, 2007.

[15] Wilfried Enkelmann et al. Fleetnet-applications for inter-vehicle communication. In *Intelligent Vehicles Symposium, 2003. Proceedings. IEEE*, pages 162–167. IEEE, 2003.

[16] Thierry Ernst et al. Network mobility support goals and requirements. IETF RFC 4886, July 2007.

[17] Gundavelli et al. Proxy mobile ipv6, IETF RFC 5213, August 2008.

[18] Masafumi Aramoto et al. Umip. *Available: http://umip.org/*, 2012.

[19] EURECOM. Openairinterface proxy mobile ipv6. *Available: http://www.openairinterface.org/components/page1103.en.htm*, 2012.

[20] Maria Fazio, Claudio Palazzi, Shirshanka Das, and Mario Gerla. Automatic ip address configuration in vanets. In *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pages 100–101. ACM, 2006.

[21] Hannes Hartenstein and Kenneth Laberteaux. *VANET: vehicular applications and inter-networking technologies*, volume 1. Wiley Online Library, 2010.

[22] The MathWorks Inc. Matlab version 7.10.0 r2010a. *Available: http://www.mathworks.com/products/matlab/*, 2010.

[23] Philippe Jacquet et al. Optimized link state routing protocol (olsr). IETF RFC 3626, October 2003.

[24] Seil Jeon, Rui Aguiar, and Behcet Sarikaya. Network mobility support using mobile mag in proxy mobile ipv6 domain. IETF draft-sijeon-netext-mmag-pmip-00, 2012.

[25] Daniel Jiang and Luca Delgrossi. Ieee 802.11 p: Towards an international standard for wireless access in vehicular environments. In *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pages 2036–2040. IEEE, 2008.

[26] David Johnson, Charles Perkins, Jari Arkko, et al. Mobility support in ipv6, 2004.

[27] Hans Kamp and Agnes Bende-Farkas. Epistemic specificity from a communication theoretic perspective. *Journal of Semantics*, 2006.

[28] James Kempf et al. Goals for network-based localized mobility management (netlmm). IETF RFC 4831, April 2007.

[29] John B Kenney. Dedicated short-range communications (dsrc) standards in the united states. *Proceedings of the IEEE*, 99(7):1162–1182, 2011.

[30] Timo Kosch, Christian J Adler, Stephan Eichler, Christoph Schroth, and Markus Strassberger. The scalability problem of vehicular ad hoc networks and how to solve it. *Wireless Communications, IEEE*, 13(5):22–28, 2006.

[31] Jong-Hyouk Lee, Thierry Ernst, and Naveen Chilamkurti. Performance analysis of pmipv6-based network mobility for intelligent transportation systems. *Vehicular Technology, IEEE Transactions on*, 61(1):74–85, 2012.

[32] Bob McQueen and Judy McQueen. *Intelligent transportation systems architectures*. Artech House Publishers, February 1999.

[33] Rui Meireles, Peter Steenkiste, and Joao Barros. Dazl: Density-aware zone-based packet forwarding in vehicular networks. In *Vehicular Networking Conference (VNC), 2012 IEEE*, pages 234–241. IEEE, 2012.

[34] Christophe J Merlin and Wendi Beth Heinzelman. A study of safety applications in vehicular networks. In *Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on*, pages 8–pp. IEEE, 2005.

[35] Mansoor Mohsin and Ravi Prakash. Ip address assignment in a mobile ad hoc network. In *MILCOM 2002. Proceedings*, volume 2, pages 856–861. IEEE, 2002.

[36] Hassnaa Moustafa and Yan Zhang. *Vehicular networks: techniques, standards, and applications*. Auerbach publications, April 2009.

[37] T. Narten, E. Nordmark, and W. Simpson. H. soliman," neighbor discovery for ip version 6 (ipv6). Technical report, RFC 4861, September, 2007.

[38] Sanket Nesargi and Ravi Prakash. Manetconf: Configuration of hosts in a mobile ad hoc network. In *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 2, pages 1059–1068. IEEE, 2002.

[39] Axel Neumann, Corinna Aichele, Marek Lindner, and Simon Wunderlich. Better approach to mobile ad-hoc networking (batman). *IETF draft-wunderlich-openmesh-manet-routing-00, October*, 2008.

[40] Filipe Neves, Andre Cardote, Ricardo Moreira, and Susana Sargento. Real-world evaluation of ieee 802.11 p for vehicular networks. In *Proceedings of the Eighth ACM international workshop on Vehicular inter-networking*, pages 89–90. ACM, 2011.

[41] FreeRADIUS Project. Freeradius client 1.1.6. *Available: http://freeradius.org/*, 2012.

[42] Lothar Stibor, Yunpeng Zang, and Hans-Jürgen Reumerman. Neighborhood evaluation of vehicular ad-hoc network using ieee 802.11 p. In *Proceedings of European Wireless Conference*, 2007.

[43] Fumio Teraoka and Tetsuya Arita. Pnemo: a network-based localized mobility management protocol for mobile networks. In *Ubiquitous and Future Networks (ICUFN), 2011 Third International Conference on*, pages 168–173. IEEE, 2011.

[44] Ajay Tirumala, Feng Qin, Jon Dugan, Jim Ferguson, and Kevin Gibbs. Iperf: The tcp/udp bandwidth measurement tool. *Available: http://dast.nlanr.net/Projects*, 2005.

[45] Asanga Udugama, Muhammad Umer Iqbal, Umar Toseef, Carmelita Goerg, Changpeng Fan, and Morten Schlaeger. Evaluation of a network based mobility management protocol: Pmipv6. In *Vehicular Technology Conference, 2009. VTC Spring 2009. IEEE 69th*, pages 1–5. IEEE, 2009.

[46] Yi Wang, Akram Ahmed, Bhaskar Krishnamachari, and Konstantinos Psounis. Ieee 802.11 p performance evaluation and protocol enhancement. In *Vehicular Electronics and Safety, 2008. ICVES 2008. IEEE International Conference on*, pages 317–322. IEEE, 2008.

[47] Mohamed Watfa. *Advances in Vehicular Ad-Hoc Networks: Developments and Challenges*. Information Science Reference, April 2010.

[48] Dan Wing. Network address translation: Extending the internet address space. *Internet Computing, IEEE*, 14(4):66–70, 2010.

[49] Kun Zhu, Dusit Niyato, Ping Wang, Ekram Hossain, and Dong In Kim. Mobility and handoff management in vehicular networks: a survey. *Wireless Communications and Mobile Computing*, pages 1–20, 2009.